8. System Management Scenario Group

The objective of the System Management Scenario Group is to demonstrate the ability of ECS system facilities and infrastructure to perform ongoing operations at the levels required for ECS Release A. The site is examined to provide assurance to the AT team of its readiness to support further acceptance testing, based on its performance under the scrutiny of the ECS Site Commission Scenario. The GSFC ECS DAAC Interfaces with the SMC, which conducts enterprise monitoring and coordination of operations for ECS managed resources. The GSFC ECS DAAC and SMC use these Interfaces to perform configuration management, security and accountability; and participate in system level problem resolution (trouble tickets). These functions use these Interfaces to provide the site management access to SMC management services and system wide data. The site-level configuration management and performance management capability is evaluated. Ancillary capabilities (fault management, security functionality, accounting and accountability, and report generation) are reviewed for functional completeness and for acceptable operation at the site, and in the total ECS system context.

8.1 ECS Site Commission Scenario

This scenario verifies the GSFC ECS DAAC procedures and the operation and care of its equipment. The scenario includes an evaluation of GSFC ECCS DAAC documented procedures, a demonstration of how its systems is "powered up", how various start-up and shutdown procedures are done, and how recovery from an abnormal shutdown is accomplished. It also demonstrates the types and availability of GSFC ECS DAAC maintenance tools and the application of approved procedures for their use. Assessment of the GSFC ECS DAAC facility interface capability includes evaluation of both external and internal interfaces.

Through a demonstration of simulated events and a policy and procedures review, confidence is built in each site's ability to successfully respond to scheduled and unscheduled events. As a final step, the AT team estimates the site's readiness to support further acceptance testing, based on the site's performance during this condensed, comprehensive overview of the systems operation.

8.1.1 M&O Procedures Review and Confidence Test Sequence

This sequence confirms the existence and completeness of documented M&O policies and procedures and confirms the correct hardware and software configuration items of the ECS site.

Configuration: The subsystem needed to perform this sequence of tests are as follows. CSS/MSS, DSS, INS, ISS, & PLS. Refer to Appendix D for additional detail.

External Interfaces: There are no external interfaces needed for this sequence.

Operator Position(s): The operator position from the ECS Maintenance and Operations Position Descriptions document (607/OP2) needed to support this sequence is listed:

DAAC Computer Operator

Operational Scenario: There are no operations scenarios, taken from the Operations Scenarios for the ECS Project: Release-A (605/OP1), used during this sequence of tests.

Test Dependencies: There are no test dependencies for this sequence.

8.1.1.1 ECS Sites Nominal Operations Policy and Procedures Review

TEST Procedure No. A080110.010$G	**Date Executed:**	**Test Conductor**
Title:	ECS Sites Nominal Operations Policy and Procedures Review	
Objective:	This test verifies the existence, accessibility and usability of documented operational and maintenance policies and procedures.	

Requirements	**Acceptance Criteria**
SMC-2605#A	This requirement is verified through demonstration. The LSM shall support the site and element in implementing ESDIS Project policies and procedures received from the SMC covering the following areas, at a minimum: a. Element responsibility and authority b. Resource management c. Fault recovery d. Testing e. Simulation f. Maintenance g. Logistics h. Performance evaluation i. Training j. Quality and product assurance k. Inventory management l. System enhancements m. Finance management n. Administrative actions o. Security The documented LSM MSS policies and procedures for the GSFC ECS DAAC must be available for use at the GSFC ECS DAAC.
Test Inputs:	Release A Version Description Document (814/) Mission Operation Procedures for the ECS Project (611/OP3)

Step-By-Step Procedures		
Step No.	**Input Action / Expected Results**	**Pass / Fail / Comments**
10	Tester: Confirms that configuration management has verified the Release A Version Description Document(DID 814) includes the following document: Mission Operation Procedures for the ECS Project(DID 611/OP3)	
20	Expected Result: Certified DID 611/OP3 is included in Release A Version Description Document (DID 814).	
30	Tester: Inspects DID 611/OP3 to verify that the following items are addressed: a. Site or element responsibility and authority b. Resource management c. Fault recovery d. Testing **e. Simulation (TBD)** f. Maintenance g. Logistics h. Performance evaluation i. Training j. Quality and product assurance k. Inventory management l. System enhancements m. Finance management n. Administrative actions o. Security	
40	Expected Result: The following items are addressed in DID 611/OP3: a. Site or element responsibility and authority b. Resource management c. Fault recovery d. Testing **e. Simulation - Section TBD** f. Maintenance g. Logistics h. Performance evaluation i. Training j. Quality and product assurance k. Inventory management l. System enhancements m. Finance management n. Administrative actions o. Security	
Data Reduction and Analysis Steps: The document DID 611/OP3 is inspected and SMC policies and procedures are verified.		
Signature:		**Date:**

8.1.1.2 ECS Hardware and Software Configuration Items Review

TEST Procedure No.: A080110.020$G	**Date Executed:**	**Test Conductor:**
Title:	ECS Hardware and Software Configuration Items Review	
Objective:	This test verifies the ECS hardware and software configuration items are on the system.	

Requirements	**Acceptance Criteria**
SMC-2515#A	This requirement is verified through test. The LSM shall provide configuration management for at least the operational hardware, system software, and scientific software within its element and for the migration of enhancements into the operational system. The Tester verifies that the Baseline Manager contains a version history of configuration controlled resources according to each site's operational baseline as described in the Release A Version Description Document (814)

Test Inputs: Release A Version Description Document (814)

Step-By-Step Procedures		
Step No.	**Input Action / Expected Results**	**Pass / Fail / Comments**
10	Tester: Check with configuration management personnel responsible for the GSFC ECS DAAC that the Release A Version Description Document (814/) lists all hardware and software configuration items configured into the system.	
20	Expected Results: Configuration management personnel certify that the Release A Version Description Document (814/) contains all the hardware and software configuration items present and properly configured into the GSFC ECS DAAC system.	
30	Computer Operator: Log into the MSS Local Management Server and execute the Baseline Manager application.	
40	Expected Results: Baseline Manager application displays on the screen.	
50	Computer Operator: Using the list of hardware and software configuration items listed in the Release A Version Description Document (814/), access and view each configuration item stored within the Baseline Manager	
60	Expected Results: Each of the configuration items listed in the Release A Version Description Document (814/) contains a. the current version; b. the current version's specifications and technical, operations, and maintenance documentation; c. the specification and technical documentation history; d. the "level of assembly" representation of the components; and e. the version history.	
70	Computer Operator: Exit the Baseline Manager.	
80	Expected Results: The screen returns to the UNIX prompt.	
Data Reduction and Analysis Steps:		
Signature:		**Date:**

8.1.2 Site Start-up Sequence

This sequence verifies the GSFC ECS DAAC can be powered up using normal cold-start procedures, operated successfully for fifteen minutes (or less if approved by the AT test conductor) and shutdown using normal shutdown procedures. The GSFC ECS DAAC is subsequently restarted to verify the system's ability to perform normal "warm restart" procedures.

During the fifteen minutes of operational time, specific configuration changes are input to the system. After normal shutdown and restart, the observed system configuration is compared to the configuration prior to shutdown to verify the preservation of system configuration parameters.

Configuration: The subsystem needed to perform this sequence of tests are as follows. CSS/MSS, DSS, INS, ISS, & PLS. Refer to Appendix D for additional detail.

External Interfaces: There are no external interfaces needed for this sequence.

Operator Position(s): The operator position from the ECS Maintenance and Operations Position Descriptions document (607/OP2) needed to support this sequence is listed:

DAAC System Administrator

Operational Scenario(s): The operations scenario, taken from the Operations Scenarios for the ECS Project: Release-A document (605/OP1), that was used to develop tests in this sequence of tests are listed:

ECS System Shutdown/Startup Scenario (Section 3.1.1)

Test Dependencies: There are no test dependencies needed for this sequence of tests.

8.1.2.1 Site Startup Confidence

TEST Procedure No.: A080110.040$G	**Date Executed:**	**Test Conductor:**
Title:	Site Startup Confidence	
Objective:	The purpose of this test is to demonstrate a normal startup, operations and shutdown of the ECS site.	

Requirements	**Acceptance Criteria**
EOSD3000#A	This requirement is verified through demonstration. The ECS shall provide for security safeguards to cover unscheduled system shutdown (aborts) and subsequent restarts, as well as for scheduled system shutdown and operational startup. System startup and shutdown must be accomplished using the cold startup and normal shutdown procedures documented in the Mission Operation Procedures for the ECS Project (611/OP3). This test does not verify unscheduled system shutdown and subsequent restarts. This is verified in 8.1.4 Site Shutdown/ Recovery Sequence.
Test Inputs:	Mission Operation Procedures for the ECS Project (611/OP3)

Step-By-Step Procedures		
Step No.	**Input Action / Expected Results**	**Pass / Fail / Comments**
	Perform an ECS cold startup in accordance with procedures documented in the Mission Operation Procedures for the ECS Project (611/OP3).	
10	System Administrator: Powers on the system components.	
20	Expected Results: System components respond. This is conveyed by power on indicator lights.	
30	System Administrator: Initializes the script to startup the system.	
40	Expected Result: Execution of the Startup Script. MSS Agent is initialized. MSS Agent calls the Client Startup Script. Client software is started. MSS Agent calls the Data Archive Subsystem Startup Script. Data Archive Subsystem is started. MSS Agent calls the Ingest Startup Script. Ingest Subsystem is started. MSS Agent calls the Data Server Startup Script. Data Server Subsystem is started. MSS Agent calls the PDPS Startup Script. PDPS Subsystem is started. MSS Agent opens the gateway to allow for incoming requests.	
50	System Administrator: Initializes HP OpenView.	
60	Expected Result: HP OpenView displays on the screen.	
70	System Administrator: Using the system management agent, configure the display to monitor a specific set of software and hardware elements.	
80	Expected Result: HP OpenView displays the specific set of elements.	
90	System Administrator: Save the configuration.	
100	Expected Results: The system management agent stores the new display configuration.	
110	System Administrator: Monitors HP OpenView to insure that all of the subsystems have been initialized.	
120	Expected Results: HP OpenView shows that each of the subsystems are up and running without any problems. This is conveyed by HP OpenView by a green icon representing each of the components.	
130	System Administrator: Sends out a message to the Computer Operators and the Resource Manager notifying them that the system is up and running.	

140	Expected Results: A pop up message is displayed on the Computer Operators' and the Resource Manager's screens.	
150	System Administrator: Monitors the system for 15 minutes.	
160	Expected Results: HP OpenView shows that each of the subsystems are up and running without any problems. This is conveyed by HP OpenView by a green icon representing each of the components.	
	Normal Shutdown	
170	System Administrator: Sends out a message to the Computer Operators and the Resource Manager notifying them that the system is going down in T-15 minutes.	
180	Expected Results: A pop up message is displayed on the Computer Operators' and the Resource Manager's screens.	
190	System Administrator: Sends out a message to the Computer Operators and the Resource Manager notifying them that the system is going down in T-10 minutes.	
200	Expected Results: A pop up message is displayed on the Computer Operators' and the Resource Manager's screens.	
210	System Administrator: Sends out a message to the Computer Operators and the Resource Manager notifying them that the system is going down in T-1 minute.	
220	Expected Results: A pop up message is displayed on the Computer Operators' and the Resource Manager's screens. At Shutdown, the system no longer allows incoming requests.	
230	System Administrator: Waits for all jobs to complete. If a job running will take longer than 10 minutes to complete the job will be stopped and the originator will be notified. Execute a "ps" command to verify that all processes have completed.	
240	Expected Results. Response to "ps" command denotes that all jobs have completed.	
250	System Administrator: Shuts down the PDPS.	
260	Expected Results: System shuts down the PDPS.	
270	System Administrator: Monitors HP OpenView to see when the PDPS has shutdown.	
280	Expected Results: The HP OpenView icon for the PDPS turns red denoting the PDPS is shutdown.	
290	System Administrator: Shuts down the Data Server.	
300	Expected Results: System shuts down the Data Server.	
310	System Administrator: Monitors HP OpenView to see when the Data Server has shutdown.	
320	Expected Results: The HP OpenView icon for the Data Server turns red denoting the Data Server is shutdown.	

330	System Administrator: Shuts down the Ingest Subsystem.	
340	Expected Results: System shuts down the Ingest. Subsystem	
350	System Administrator: Monitors HP OpenView to see when the Ingest Subsystem has shutdown.	
360	Expected Results: The HP OpenView icon for the Ingest Subsystem turns red denoting the Ingest is shutdown.	
370	System Administrator: Shuts down the Data Archive Subsystem.	
380	Expected Results: System shuts down the Data Archive Subsystem.	
390	System Administrator: Monitors HP OpenView to see when the Data Archive Subsystem has shutdown.	
400	Expected Results: The HP OpenView icon for the Data Archive Subsystem turns red denoting the Data Archive is shutdown.	
410	System Administrator: Shuts down the Client software.	
420	Expected Results: System shuts down the Client software.	
430	System Administrator: Monitors HP OpenView to see when the Client software has shutdown.	
440	Expected Results: The HP OpenView icon for the Client software turns red denoting the Client software is shutdown.	
450	System Administrator: Shuts down the MSS Subsystem.	
460	Expected Results: System shuts down the MSS Subsystem and the UNIX prompt appears.	
Data Reduction and Analysis Steps:		
Signature:		**Date:**

8.1.2.2 Site Restart Including Introduction of Previous Results

TEST Procedure No.: A080120.010$G	**Date Executed:**	**Test Conductor:**
Title:	Site Restart Including Introduction of Previous Results	
Objective:	This test demonstrates the ability of the ECS to perform a warm restart and demonstrates that configuration inputs from the prior operational state are still active following a shutdown and restart process.	

Requirements	**Acceptance Criteria**
EOSD3000#A	This requirement is verified though demonstration. The ECS shall provide for security safeguards to cover unscheduled system shutdown (aborts) and subsequent restarts, as well as for scheduled system shutdown and operational startup. The ECS must perform a warm restart and demonstrate the return to the preserved configuration from the previous operational state. This test does not verify "unscheduled system shutdown (aborts) and subsequent restarts" and "scheduled system shutdown. They are verified in 8.1.4 Site Shutdown/Recovery Sequence and 8.1.2.1 Site Startup Confidence Test respectively.
Test Inputs:	Mission Operation Procedures for the ECS Project (611/OP3)

Step-By-Step Procedures		
Step No.	**Input Action / Expected Results**	**Pass / Fail / Comments**
	Perform an ECS warm restart in accordance with procedures documented in the Mission Operation Procedures for the ECS Project (611/OP3).	
10	System Administrator: Initializes the script to startup the system.	
20	Expected Result: Execution of the Startup Script. MSS Agent is initialized. MSS Agent calls the Client Startup Script. Client software is started. MSS Agent calls the Data Archive Subsystem Startup Script. Data Archive Subsystem is started. MSS Agent calls the Ingest Startup Script. Ingest Subsystem is started. MSS Agent calls the Data Server Startup Script. Data Server Subsystem is started. MSS Agent calls the PDPS Startup Script. PDPS Subsystem is started. MSS Agent opens the gateway to allow for incoming requests	
30	System Administrator: Initializes HP OpenView.	
40	Expected Result: HP OpenView displays on the screen.	
50	System Administrator: Verifies that the configuration saved in test 8.1.2.1, step 90 is displayed on the screen.	
60	Expected Results: HP OpenView shows that each of the subsystems are up and running without any problems. This is conveyed by HP OpenView by a green icon representing each of the components.	
70	System Administrator: Sends out a message to the Computer Operators and the Resource Manager notifying them that the system is up and running.	
80	Expected Results: A pop up message is displayed on the Computer Operators' and the Resource Manager's screens.	
90	System Administrator: Monitors the system for 15 minutes.	

100	Expected Results: HP OpenView shows that each of the subsystems are up and running without any problems. This is conveyed by HP OpenView by a green icon representing each of the components.	
Data Reduction and Analysis Steps:		
Signature:		**Date:**

8.1.3 Site Operations Sequence

This sequence is not valid for the GSFC ECS DAAC Volume of the Acceptance Test Procedures document for Release A.

8.1.4 Site Shutdown/Recovery Sequence

This sequence evaluates the capability of the ECS site to perform documented emergency shutdown procedures. This sequence also evaluates the capability of the ECS site to recover from the abnormal shutdown and to provide continued performance, albeit in a degraded mode, during a device failure. A device failure is simulated during the restart process by forcing the RAID storage device to go off-line.

Configuration: The subsystem needed to perform this sequence of tests are as follows. CSS/MSS, DSS, INS, ISS, & PLS. Refer to Appendix D for additional detail.

External Interfaces: There are no external interfaces needed for this sequence.

Operator Position(s): The operator positions from the ECS Maintenance and Operations Position Descriptions document (607/OP2) needed to support this sequence are listed:

DAAC Computer Operator

DAAC System Administrator

DAAC Resource Manager

DAAC Production Monitor

Operational Scenario(s): The operations scenario, taken from the Operations Scenarios for the ECS Project: Release-A document (605/OP1), that was used to develop tests in this sequence of tests are listed:

Computer System Administration Backup & Restore/Recovery (Section 3.1.2)

Test Dependencies: The following table identifies the test procedure(s) in a sequence of tests that should be run prior to or concurrently with a sequence or test procedure.

Test Procedure No.	Site/Procedure No.	Comments
A080140.010$G A080150.010$G A080150.020$G	A080170.020$G	Run A080170.020$G prior to any test in this sequence.
A080140.010$G A080150.010$G A080150.020$G	A080180.090$G	Run A080180.090$G prior to any test in this sequence.
A080150.010$G	A080620.040$G	Run A080620.040$G prior to A080150.010$G

8.1.4.1 Emergency and Other Abnormal Shutdown

TEST Procedure No.:	**Date Executed:**	**Test Conductor:**
A080140.010$G		Dawn El Missouab

Title:	Emergency and Other Abnormal Shutdown
Objective:	This confirms that the site's standard procedures contain methodology for responding to catastrophic situations that require immediate site shutdown and for other types of abnormal shutdown such as system critical equipment failure.

Requirements	**Acceptance Criteria**
EOSD3000#A	This requirement is verified through demonstration. The ECS shall provide for security safeguards to cover unscheduled system shutdown (aborts) and subsequent restarts, as well as for scheduled system shutdown and operational startup. The emergency shutdown of the ECS must be accomplished using the procedures documented in the Operator's Manual. This test does not verify “subsequent restarts, as well as for scheduled system shutdown and operational startup”, are not verified in this procedure and are verified in 8.1.2 Site Startup Sequence

Test Inputs: Mission Operation Procedures for the ECS Project (611/OP3)

Data Set Name	**Data Set ID**	**File Name**	**Description**	**Version**
		BadCfgFile	Bad Configuration File	

Step-By-Step Procedures		
Step No.	**Input Action / Expected Results**	**Pass / Fail / Comments**
10	Computer Operator: Perform an emergency shutdown in accordance with procedures documented in the Mission Operation Procedures for the ECS Project (611/OP3).	
20	Expected Results: The system is in the shut down state where each subsystem is offline. **A more detailed description of the shutdown state will be incorporated upon completion of the Mission Operation Procedures for the ECS Project (611/OP3).**	
Data Reduction and Analysis Steps:		
Signature:		**Date:**

8.1.4.2 Recovery From Catastrophic Emergency Shutdown

TEST Procedure No.:	**Date Executed:**	**Test Conductor:**
A080150.010$G		Dawn El Missouab
Title:	Recovery From Catastrophic Emergency Shutdown	
Objective:	The purpose of this test is to verify the ECS site can recover from an emergency shutdown and that the FSMS can continue to provide service in the event of a device failure.	

Requirements	**Acceptance Criteria**
DADS1540#A	This requirement is verified through demonstration. In case of corruption or catastrophic failure, capabilities for recovering the file directory shall be provided. The DADS must be able to restore files after a catastrophic failure. This test does not verify data corruption. This is verified in 8.1.4.3 Recovery From Abnormal Non-Catastrophic Shutdown.
EOSD2990#A	This requirement is verified through demonstration. The ECS elements shall support the recovery from a system failure due to a loss in the integrity of the ECS data or a catastrophic violation of the security system. The system must be able to restore files following a simulated catastrophic violation of the security system. This test does not verify "...the recovery from a system failure due to a loss in the integrity of the ECS data…". This is verified 8.1.4.3 Recovery From Abnormal Non-Catastrophic Shutdown.
EOSD3000#A	This requirement is verified through demonstration. The ECS shall provide for security safeguards to cover unscheduled system shutdown (aborts) and subsequent restarts, as well as for scheduled system shutdown and operational startup. The system must be able to restore files following a simulated catastrophic violation of the security system. This test does not verify "unscheduled system shutdown (aborts)" and "scheduled system shutdown and operational startup." They are verified in 8.1.4.1 Emergency and Other Abnormal Shutdown and 8.1.2 Site Startup Sequence respectively.

Test Inputs: Operator's Manual

Step-By-Step Procedures		
Step No.	**Input Action / Expected Results**	**Pass / Fail / Comments**
	NOTE **A080620.040$G must be run prior to this test.**	
10	Computer Operator: Attempts to bring the system back on-line, but discovers that some key files are missing.	
20	Expected Results: A file listing of the system does not contain the key files.	
30	Computer Operator: Determines that a full restore of the system files from a previous backup will fix the problem. Enters the commands to initialize the scripts to begin the restore.	
40	Expected Results: System initializes the scripts to restore the software.	
50	Computer Operator: Invokes the word processor and moves to the backup directory, to review the log file associated with the backup being restored.	
60	Expected Results: System displays the log file on terminal.	
70	Computer Operator: Selects the backupxxxxxx.log file (where xxxxxx represents the month, day, and year of the backup).	
80	Expected Results: System displays appropriate log file.	
90	Computer Operator: Prints out a copy of the log file.	
100	Expected Results: Prints the log file.	
110	Computer Operator: Exits the log file directory.	
120	Expected Results: System returns to word processor. Restore concludes and an indicator is returned to the operator.	
130	Computer Operator: From the word processor that is already up, opens the file pull down menu and selects open. Then, opens the associated QA report.	
140	Expected Results: System displays the QA report.	
150	Computer Operator: Compares the QA report with the log file from the backup that was restored.	
160	Expected Results the QA report and the log file list the same files.	
170	System Administrator: Initializes the script to startup the system as described in the Mission Operation Procedures for the ECS Project (611/OP3).	
180	Expected Results: HP OpenView shows that each of the subsystems are up and running without any problems. This is conveyed by HP OpenView by a green icon representing each of the components.	

Data Reduction and Analysis Steps:	
a. The following are secured for analysis at the close of the procedure: 1. Backup log. 2. QA report. b. Verify the QA report confirms the contents of the files restored from the archive media (listed on the backup log.	
Signature:	**Date:**

8.1.4.3 Recovery From Abnormal Non-Catastrophic Shutdown

TEST Procedure No.: A080150.020$G	**Date Executed:**	**Test Conductor:**
Title:	Recovery From Abnormal Non-Catastrophic Shutdown	
Objective:	This test confirms the sites ability to restore files caused by an abnormal non-catastrophic shutdown using standard operational procedures and that the FSMS can continue to provide service in the event of a device failure.	

Requirements	Acceptance Criteria
DADS1540#A	This requirement is verified through demonstration. In case of corruption or catastrophic failure, capabilities for recovering the file directory shall be provided. The DADS must be able to restore files corrupted by a FSMS failure. This test does not verify catastrophic failures. This is verified in 8.1.4.2 Recovery From Catastrophic Emergency Shutdown.
DADS1610#A	This requirement is verified through demonstration. The FSMS shall provide for continued performance, albeit in a degraded mode, when a device (e.g., disk or cartridge drive, operator's console) fails. The ECS FSMS must be able to provide continued service to a registered science user during a simulated failure of the RAID storage device.
DADS1630#A	This requirement is verified through demonstration. At each DADS, tools shall be provided for recovery of data from failed media and devices. The DADS must be able to restore file from a previously made backup of the archive media.
DADS2276#A	This requirement is verified through demonstration. Each DADS shall have the capability to restore its archive by storing a backup copy of EOS data or backup copy of information required to regenerate the data. The DADS must be able to restore a file(s) from a previously made backup of the archive media.
DADS2300#A	This requirement is verified through demonstration. Each DADS shall provide a capability for local and offsite backup/restore of system files. The DADS must be able to restore a file(s) from a previously made backup of the archive media.
DADS2950#A	This requirement is verified through demonstration. In case of failure of the automated system, archive media shall be capable of being manually mounted at each DADS. The archive media resident in storage devices must be manually accessible and mountable.
EOSD2440#A	This requirement is verified through test. Data base integrity including prevention of data loss and corruption shall be maintained. The DADS must be able to restore files corrupted by a FSMS failure.
EOSD2990#A	This requirement is verified by demonstration.

	The ECS elements shall support the recovery from a system failure due to a loss in the integrity of the ECS data or a catastrophic violation of the security system. The DADS must be able to restore files following a simulated catastrophic failure.
Test Inputs: Mission Operation Procedures for the ECS Project (611/OP3)	

Step-By-Step Procedures		
Step No.	**Input Action / Expected Results**	**Pass / Fail / Comments**
10	Computer Operator: Executes a simulated FSMS Server Host disc crash. Views HP OpenView.	
20	Expected Result: The GSFC icon in HP OpenView is red.	
30	Computer Operator: Double clicks on the GSFC icon to go down to the next level of submaps.	
40	Expected Result: The GSFC submap displays on the screen. The DRPHW-GSFC-1 icon is red.	
50	Computer Operator: Double clicks on the DRPHW-GSFC-1 icon to go down to the next level of submaps.	
60	Expected Result: The DRPHW-GSFC-1 submap displays on the screen. The disk drive icon is red.	
70	Computer Operator: Tries to write to the disk and fails. Then, determines the disk has failed.	
80	Expected Results: The disk cannot be written to.	
90	Computer Operator: Initiate the archive media recovery utility (Need to research if and how the SQL build master recovery utility or other recovery utilities will be implemented in GSFC Release A).	
100	Computer Operator: Schedules the replacement and restore of the disk with the Resource Manager and the Production Monitor.	
110	Expected Results: Based on the resources needed and the time required to conduct the restore the event is scheduled.	
120	Computer Operator: Notifies all affected users that the system has crashed and a restore is scheduled for 0100. This message also indicates which date the backup that will be used was taken.	
130	Expected Results: System sends e-mail.	
140	Computer Operator: Retrieves the backup which is stored in a different facility. Enters the commands to initialize the scripts to begin the restore.	
150	Expected Results: System initializes the scripts to restore the FSMS Server Host disc.	
160	Computer Operator: Invokes the word processor and selects "Open" from the file pull down menu to review the log file associated with the backup being restored.	
170	Expected Results: System displays the log file on the terminal.	
180	Computer Operator: Selects the Restorexxxxxx.log (where xxxxxx equal the month, day and year).	
190	Expected Results: System displays appropriate log file.	
200	Computer Operator: Prints out a copy of the log file.	

210	Expected Results: Prints the log file.	
220	Computer Operator: Exits the log file directory.	
230	Expected Results: System returns to word processor. Restore concludes and an indicator is returned to the operator.	
240	Computer Operator: Restores the incremental backups taken since the last system backup to bring the system as close to realtime as possible.	
250	Expected Results: The restores conclude and an indicator is returned to the operator.	
260	Computer Operator: From the word processor that is already up, the QA report associated with the restore.	
270	Expected Results: System displays the QA report.	
280	Computer Operator: Compares the QA report with the log file from the backup that was restored.	
290	Expected Results the QA report and the log file list the same files.	
300	Computer Operator: verifies that the system is back up and operational.	
310	Expected Results: HP OpenView shows that the GSFC icon is up and running without any problems. This is conveyed by HP OpenView by a green icon.	
320	Computer Operator: Notifies the affected users that the restore has concluded and that activities that were performed before Day 5 at 1900 may need to be redone.	

Data Reduction and Analysis Steps:

a. The following are secured for analysis at the close of the procedure:

1. Backup log.
2. QA report.

b. Verify the QA report confirms the contents of the files restored from the archive media (listed on the backup log.

Signature:	**Date:**

8.1.5 Site Maintenance Sequence

The Site Maintenance sequence is composed demonstrations of maintenance and operations (M&O) tools at Release A sites. The primary purpose is to assure that the staff can access M&O services, via appropriate interfaces, allowing them to select the correct M&O interface to ECS subsystems from local and remote terminals. ECS functions requiring an M&O interface are system management, science algorithm integration, product generation, data archiving and distribution, user support services and system maintenance.

Configuration: The subsystem needed to perform this sequence of tests are as follows. CSS/MSS, DSS, INS, ISS, & PLS. Refer to Appendix D for additional detail.

External Interfaces: The external interface (i.e. other ECS sites and data sources) needed for this sequence (both real and simulated) is listed:

SMC

LaRC DAAC

Operator Position(s): The operator positions from the ECS Maintenance and Operations Position Descriptions (607/OP2) document needed to support this sequence are listed:

DAAC Operations Supervisor

DAAC Resource Manager

DAAC Archive Manager

DAAC Computer Operator

DAAC User Services Representative

DAAC Ingest Distribution Technician

Operator Scenario: There are no operations scenarios, taken from the Operations Scenarios for the ECS Project: Release-A (605/OP1), used during this sequence of tests.

Test Dependencies: There are no test dependencies needed for this sequence of tests.

8.1.5.1 DAAC M&O Interfaces

TEST Procedure No.: A080160.010$G	**Date Executed:**	**Test Conductor:**
Title:	DAAC M&O Interfaces	
Objectives:	Demonstrate that M&O interfaces, provided for GSFC DAAC ECS subsystems are accessible and functioning and that these interfaces are sufficient to support planned operations and maintenance activities. Demonstrate that the M&O interface provides access to on-line services for Accountability, Fault Management, Performance Management, and Report Generation. Demonstrate that other on-line services are available for three aspects of security management network, communications and host processors along with general message exchange services to support E-mail, FTP file access, Bulletin Board, and Virtual Terminal capabilities. Demonstrate that the M&O interface provides access to off-line configuration control services to support Baseline Management, S/W Change Management, Change Request Management, S/W Distribution Management, and S/W License Management, Demonstrate that the M&O interface provides access to off-line resource management services to support Inventory management, Logistics management, Training and Policies & Procedures management using Office Automation tools.	

Requirements	**Acceptance Criteria**
EOSD1 703#A	This requirement is verified through demonstration. The system shall provide M&O interfaces which support the functions of: a. System Management, b. Science Algorithm Integration,

	c. Product Generation, d. Data Archive/Distribution, e. User Support Services, and f. System Maintenance. M&O interfaces must provide system management functionality with links to Accountability Services, Management Data Access services and Fault Management services. Fault Management Services must provide access to external systems, interfaces with management agents, Performance Management Services, Security services, M&O system management interfaces must include links to CSS and system log. The interfaces must provide access to AI&T team data, and Bulletin Board(s) via ECS workstations using Virtual Terminals. M&O interfaces must provide initialization, recovery and orderly shutdown for the following CIs SPRHW, AITHW, ICLHW, AND PLNHW.

Test Inputs:

Data Set Name	Data Set ID	File Name	Description	Version
Accountability Registered Users (principal)				
Access Control List (GSFC)				
Host Authentication database				
User Profiles				
User Audit Trial				
Data Product Audit Trail				
DCE registry database				
Router configuration database				

Step-By-Step Procedures		
Step No.	**Input Action / Expected Results**	**Pass / Fail / Comments**
	M&O Staff Interface	
	Use MSS services to demonstrate M&O interface capabilities and services.	
100	Computer Operator: Uses MSS M&O interface services and selects an option to create an ECS user account.	
120	Expected Results: System provides screen(s), APIs and Icons which allow Computer Operator to create a principal ECS Science Group Account.	
120	Computer Operator: Uses screen input fields, APIs and Icons to create and submit an ECS Science Principal Group Account.	
121	Expected Results: System provides display, confirmation status indicators and messages verifying that an ECS science principal group account has been created.	
130	Computer Operator: Uses MSS M&O interface services and selects an option to add or update a user's profile information within the newly created ECS Science Principal Group Account.	
131	Expected Results: System provides screen(s), APIs and Icons that allow Computer Operator to add or update user profile information.	
140	Computer Operator: Uses screen input fields, APIs and Icons to add or update and then submit modification(s) to user profile information.	
141	Expected Results: System provides display and confirmation status indicators and messages verifying that user profile information has been added or updated.	
142	User Services Representative: Logs on using the ECS Science Principal Group Account that has been created.	
143	Expected Results: System responds and the User Services Representative is free to begin working within the account.	
144	User Services Representative: Invokes the word processor and selects “Open” from the file pull down menu to review a file.	
145	Expected Results: System displays the file on the terminal.	
146	User Services Representative: Exits the word processor.	
147	Expected Results: Word processor closes and returns to the MSS M&O interface services screen.	
150	Computer Operator: Uses MSS M&O interface services and selects an options to locate and delete a user's profile information from an ECS science users group account.	
151	Expected Results: System provides screen(s), APIs and Icons which allow Computer Operator to delete a user's profile information from a principal ECS science Group account.	

160	Computer Operator: Uses screen input fields, APIs and Icons identify the account and user for deletion. Then submits a delete requests for one user's profile information within an ECS science principal group account.	
161	Expected Results: System provides display and confirmation status messages which indicates that the selected user profile information, within an ECS science principal group account, has been deleted.	
170	Computer Operator: Uses screen input fields, APIs and Icons to identify an ECS science principal account for deletion. Then submits a delete requests for an ECS Science Principal Group Account.	
171	Expected Results: System provides screen(s), APIs and Icons which allow Computer Operator to delete a principal ECS Science Group Account.	
180	Computer Operator: Uses screen input fields, APIs and Icons to identify the ECS science principal group account for deletion. Then submits a delete request for one ECS science principal group account.	
181	Expected Results: System provides display and confirmation status messages which indicates that the selected ECS science principal group account, has been deleted.	
190	Computer Operator: Use M&O interface services to demonstrate capability to construct and execute an inquiry for all profile information for a principal ECS science user group.	
191	Expected Results: System provide screen(s), APIs, data input fields and Icons that allow Computer Operator to formulate and submit an inquiry for a specific user's profile information.	
192	Expected Results: System provides display and confirmation status for the user profile inquiry. User profile information consist of: User ID, name, home DAAC, contact phone number(s) e-mail information, organization, research field, affiliation, sponsor, project name, Principal Investigator, alternate mail address, account number, billing information, privilege levels and creation and expiration dates.	
200	Computer Operator: Uses MSS M&O interface services and selects options to perform an inquiry for a users order status.	
201	Expected Results: System provide screen(s), APIs, data input and Icons that allow Computer Operator to input an inquiry for a user's order status.	
210	Expected Results: System provides display, confirmation status messages and order status data. Order status information consist of: user id, name and address, distribution format, distribution lists, media, size, granule information, home DAAC, ship and billing information, file name(s), submission dates and times, finish date and time, status time of last update.	
211	Expected Results: System reruns Order status information containing user id, name and address, distribution format, distribution lists, media, size, granule information, home	

	DAAC, ship and billing information, file name(s), submission dates and times, finish date and time, status time of last update.	
	Demonstrate M&O interface capability to formulate and execute an inquiry to acquire a user's account History.	
220	Expected Results: System provide screen(s), APIs, data input fields and interactive Icons at the accountability services interface that allow Computer Operator to formulate and submit an inquiry for a specific user's account History.	
222	Expected Results: System provides display, confirmation status messages and account history data. Account History consist of: Pending requests, approved requests, subsets of registered users, and subsets of user profile information within principal ECS user groups.	
230	Archive Manager: Demonstrate M&O Interface capability to formulate and execute an inquiry to acquire a user's account status.	
231	Expected Results: System provide screen(s), APIs, data input fields and interactive Icons at the M&O Interface services interface that allow Computer Operator to formulate and submit an inquiry for a specific user 's account Status.	
	Use M&O Staff interface to demonstrate Accountability Manager Application Services to perform GSFC User Registration.	
310	Archive Manager: Demonstrate M&O staff interface capability to Create user profile information.	
311	Expected Results: System provide screen(s), APIs, data input fields and interactive Icons at the M&O interface that allow Computer Operator to create a specific user's profile.	
320	Archive Manager: Demonstrate M&O Staff interface capability to modify user profile information.	
321	Expected Results: Demonstrate M&O staff interface capability to construct a query to audit the order Status, specify time period and format for a principal ECS science user group.	
340	Operations Supervisor: Demonstrate M&O staff interface capability to delete user Profile information	
341	Expected Results: System provides status messages, and reports/Displays indicating that identified user profile information is deleted from active profile database. Attempts to acquire resource usage or request status will result in audit trail and log entries indicating that user(s) profile information is not available.	
	Use M&O Staff Interface to access and demonstrate Accountability Manager Application Service that includes access to management Data Access interface to support Audit Trail activity	
350	Operations Supervisor: Demonstrate accountability manager interface capability to construct a query to audit the order status, specify time period and format for a principal ECS science user group	

351	Expected Results: System provides data audit trail reports and displays. Displays/Reports consists of data provided to uses. Reports are ordered by data type. Information contains unique identifiers of serve transaction and/or request(s), host address, date(s) of request(s), time of request(s), and brief description of system access activities, i.e., process or application initiating request, start actions end actions, version information and unique ID of service(s).	
360	Operations Supervisor: Demonstrate accountability manager interface capability to construct a query to audit the account history, specify time period and format for a user within a principal ECS science users group.	
361	Expected Results: System provides user audit trail reports and displays. Displays/Reports consists of history of registered user data detailing unique identifiers of serve transaction and/or request(s), host address, date(s) of request(s), time of request(s), and brief description of system access activities, i.e., process or application initiating request, start actions end actions, version information and unique ID of service(s).	
370	Archive Manager: Demonstrate accountability manager interface capability to execute a query for an audit of user's account status, specify time period and format for a user within a principal ECS Science Users Group.	
371	Expected Results: System provides user audit trail reports and displays. Displays/Reports consists of registered user data detailing unique identifiers of serve transaction and/or request(s), host address, date(s) of request(s), time of request(s), and brief description of system access activities, i.e., process or application initiating request, start actions end actions, version information and unique ID of service(s).	
380	Resource Manager: Demonstrate accountability manager interface capability to execute a query to analyze an audit a user's account, specify time period and format for a principal ECS science users group. two part report ordered by 1 or more parameters such as request date range, organization, research field, file name (instrument or event) etc. user audit analysis report consist of: user id, name, e-mail address, organization, research field, affiliation, project, principal investigator. data audit analysis report consist of: product order request history, submission date and time, finish times, file name(s), shipping and billing information, resources utilization.	
381	Expected Results: System returns displays and/or produces reports ordered by 1 or more parameters such as request date range, organization, research field, file name (instrument or event) etc.. user audit contains user audit analysis report consist of: user id, name, e-mail address, organization, research field, affiliation, project, principal investigator, and data audit analysis displays and/or reports containing	

	product order request history, submission date and time, finish times, file name(s), shipping and billing information, resources utilization.	
400	Resource Manager: Use MSS M&O staff interface to demonstrate system management services for policy management using office automation services. (o/a)	
401	Expected Results: System provides access to data base spread sheets, bulletin boards, and web pages of SMC policies and directives	
410	Resource Manager: Use MSS M&O staff interface to demonstrate system management services for fault management using COTS (HP OpenView).	
411	Expected Results: System provides access to an interface for MSS fault management services.	
	Use MSS M&O staff interface to demonstrate CM services for file access services for ECS management data, science data, science metadata along with site operations for SDPS planning and scheduling information. (CM & file access service)	
421	Expected Results: System provide access to interfaces which facilitate CM services with capabilities to use file access services to acquire ECS management data, science data, science metadata along with site operations for SDPS planning and scheduling information. (CM & file access service)	
430	Resource Manager: Use MSS M&O staff interface to demonstrate services to access CM cots on GSFC DAAC ECS workstation(s) and virtual terminals .	
431	Expected Results: System provides access to an interface for MSS configuration management application services.	
440	Resource Manager: Use MSS M&O staff interfaces to demonstrate CM tool services for ECS s/w change activities.	
441	Expected Results: System provides access to an interface for MSS configuration management application services. (CM)	
500	Resource Manager: Use MSS M&O Interfaces to demonstrate CM tool services for ECS S/W Merge activities.	
501	Expected Results: System provides interface to CM management tools and services which allow Computer Operator acquire and merge builds of ECS software. The software mix can be custom and COTS.	
510	Resource manager: Use MSS M&0 Staff Interfaces to demonstrate CM tool services for ECS S/W directory management and updates.	
511	Expected Results: System provides interface to CM management tools and services which allow Computer Operator perform directory maintenance as part of site maintenance activities.	
520	Resource Manager: Use MSS M&O staff Interfaces to demonstrate CM tool services to send and receive e-mail, and update Bulletin Boards. (E-mail, Bulletin Board).	
521	Expected Results: System provides interface to CM	

	management tools and services which allow Computer Operator access e-mail serves and Bulletin board services.	
530	Resource Manager: Use Baseline Management tools/services to acquire ECS S/W licensing information and produce reports for the DAAC's S/W and H/W baseline configuration(s). (Baseline Manager)	
531	Expected Results: System provides interface to CM management tools and services which allow Computer Operator access and perform services site baseline management (XRP II).	
540	Resource Manager: Use MSS M&0 Staff Interfaces to demonstrate CM tool services for Change Request Management activities (DDTS).	
541	Expected Results: System provides interface to CM management tools and services which allow Computer Operator access and perform services site chug request management VCATS and ClearCase and, (XRP II).	
600	Ingest Distribution Technician: Use MSS M&0 Staff Interfaces to demonstrate system management services for Performance Management.	
601	Expected Results: System provides interface to MSS management application services and tools which allow Computer Operator access and perform Site Performance Management activities (HPOV Perform. MGT Report Gen.)	
	Use MSS M&0 Staff Interfaces to demonstrate services for Trouble Ticketing.	
610	Expected Results: system provides interface to MSS management application services and tools which allow Computer Operator access and perform Trouble Ticket Management activities (Remedy).	
620	DAAC Security Administration Analyst: Use MSS M&0 Staff Interfaces to demonstrate services for Security Management.	
621	Expected Results: System provides interface to MSS and CSS management application services and tools which allow Computer Operator to access and perform Site Security Management activities.	
630	Resource Manager: Use MSS M&0 Staff Interfaces to demonstrate services for Inventory, Logistics and Maintenance.	
631	Expected Results: TBS	
Data Reduction and Analysis Steps:		
Signature:		**Date:**

8.1.5.2 Maintenance of ECS Databases

TEST Procedure No.: A080160.020$G	**Date Executed:**	**Test Conductor**
Title:	Maintenance of ECS Databases	
Objective:	Demonstrate that interfaces between the ECS Subsystem Servers and their respective M&O Administrative terminal(s) will support Maintenance of ECS Data bases. Demonstrate that maintenance of ECS DBs do not require a "change" of display screens after modification of database structures provided by ECS DB servers. Demonstrate capabilities to interrupt maintenance session and restart the session without loss of information. Verify through Inspection that GSFC LSM database maintenance capabilities reflect cross site standards for maintenance of ECS Databases. The procedure assures that the procedures are available, current, and complete.	

Requirements	Acceptance Criteria
IMS-0170#A	This requirement is verified through demonstration. The IMS user interface must be designed so that restructuring of IMS data bases shall not result in the need for changes to the IMS interface. Demonstrate ESDT DB restructuring activities using interfaces between SDSVR CSCI and the SDSVR ADMIN/OPS terminal. Demonstrate Advertising DB restructuring activities using interfaces between ADSVR CSCI and the ADSVR ADMIN/OPS terminal. Demonstrate Dictionary DB restructuring activities using interfaces between DDICT CSCI and the DDICT ADMIN/OPS terminal. DB schema updates do not require Admin staff to change or otherwise re-select "view" screens to confirm schemata update results.
IMS-0210#A	This requirement is verified through demonstration. The IMS shall allow data access privileges to be configurable by user and data type for: a. Read b. Write c. Update d. Delete e. Any combination of the above The Tester must be able to log on to a user account and reconfigure account privileges.
IMS-0220#A	The requirement is verified through demonstration. The IMS shall store, maintain and provide data management services for ECS directory, inventory, and guide (documentation/reference material) and other IMS data bases. The Tester must be able to store, maintain and access data management services for ECS directory, inventory, and guide databases.
IMS-0230#A	The requirement is verified through demonstration. The IMS shall restrict update of ECS directory, inventory, and guide (documentation/reference material) and other IMS data bases to authorized users based on the users access privileges. Only authorized users with valid passwords are able to logon to ECS and update ECS directory, inventory, and guide (documentation/reference material) and other IMS data bases.

IMS-0240#A	The requirement is verified through demonstration. The IMS shall provide, at a minimum, database administration utilities for: a. modification of ECS database schema, b. performance monitoring, c. performance tuning, d. administration of user access control, e. perform on-line incremental backup, f. perform on-line recovery, and g. export/import of data. Demonstrate that once a DB administration utility session is established, it's capabilities and services are segmented and exercised in a mutually exclusive fashion. Demonstrate that any combination of (a) through (g) can be exercised concurrently on a single Operations workstation or across multiple workstations.
IMS-0250#A	This requirement is verified through demonstration. The IMS shall provide required maintenance of the IMS data bases, to include at a minimum: a. Capability to restructure the data base b. Capability to interrupt a maintenance session and restart the session without loss of information. The Tester must be able to restructure the database and restart without loss of information following an interruption of a maintenance session.
IMS-0260#A	This requirement is verified through demonstration. The IMS must provide interactive and batch information management capabilities for authorized users to add, update, delete and retrieve information from the ECS data databases. Demonstrate capabilities for authorized personnel to access and use DB administration services in both batch and interactive modes of operation. Demonstrate capability to submit batch tasks which accomplish DB updates, DB deletions and DB retrievals to/from ECS data resources. Demonstrate capability to interactively control tasks to accomplish DB updates, DB deletions and DB retrievals to/from ECS data resources.
IMS-0290#A	This requirement is verified through demonstration. IMS internal data base management queries shall be expressed in a standard query language (SQL). Demonstrate database management queries written in SQL. **Change method from analysis to demonstration in CCR.**
IMS-0350#A	This requirement is verified through demonstration. The IMS shall provide capability for authorized personnel to add, delete, or modify ECS metadata entries, individually or in groups. Demonstrate capabilities for authorized personnel to access and use DB administration services. Personnel demonstrate capability to add, delete or modify ECS metadata entries (individual or group) based on ownership.

	Demonstrate capabilities for authorized personnel to access and use DB administration services. Personnel demonstrate capability to add, delete or modify ECS metadata entries (individual or group) based data types. Demonstrate capabilities for authorized personnel to access and use DB administration services. Personnel demonstrate capability to add, delete or modify ECS metadata entries (individual or group) based on privileges. **Verification in RTM Inspection. Method changed to demonstration. Requires update pending CCR.**

Test Inputs:

Data Set Name	Data Set ID	File Name	Description	Version
Registered Users (principal)			Principal users by organization (ECS/Non-ECS)	
Access Control List (GSFC)			Access to ECS resources with account links	
Authentication's			Authentication's and Authorization of ECS service operations by group and user.	
User Profiles			Contact information, affiliations, sponsor, account number, shipping and billing , privileges, expiration date, e-mail etc..	
Advertising Service DB			Advertising Service DB Collection and Schema	
Science Data Server ESDT DB			Science Data Server ESDT DB Collection and Schema	
Data Dictionary Server Dictionary DB			Data Dictionary Server Dictionary DB Collection and Schema	

Step-By-Step Procedures		
Step No.	**Input Action / Expected Results**	**Pass/Fail/Comments**
	Science Data Server (SDSVR) CSCI	
100	Computer Operator: Initialize a SDSVR CSCI, establishes an Admin. session, selects the ESDT DB schema update function, and configures the SDSVR schema update function to monitor the status of the session.	
105	Expected Results: The selected SDSVR CSCI is available, an Admin/Ops session is established, the ESDT DBschemata update function provides a default screen for viewing ESDT DB schema information, and there are no errors resulting from the session establishment.	
110	Computer Operator: Select an ESDT DB collection and a schema within that collection to update.	
115	Expected Results: Session remains established, Computer Operator does not select a new display to "View" the schemata, no status error from selection actions is presented and the Schema is returned and displayed for update.	
120	Computer Operator: Monitor the Update status indicators and performs the data entry to update the schema.	
125	Expected Results: Session remains established, Computer Operator does not select a new display to "View" the schemata, no errors from the update actions are presented and the Schema remains displayed while Computer Operator reviews his/her update inputs.	
130	Computer Operator: Monitors the Update service status indicators, request status of the schema update be provided by the service, and submit the schemata update to the SDSVR.	
135	Expected Results: Session remains established, Computer Operator does not select a new display to "View" the schemata, no errors from the submit actions are presented in status messages.	
140	Computer Operator: Monitors the Update service status indicators and request status of the schema update submit be provided by the ESDT DB Schema Update service.	
145	Expected Results: Session remains established, Computer Operator does not select a new display to "View" the schema, status message(s) indicate that selected ESDT DB collection schema has been accepted and updated, no errors from the accept and update actions are presented in status messages, "new" ESDT DB collection schema is presented without having to change the update service "view" screen(s). Schema contains all updates entered by the tester	
150	Computer Operator: Monitors service status indicators for schema update activities and request SDSRV Admin. service to terminate both the ESDT DB Schemata update and Admin. service sessions.	

	Advertising Data Server (ADSVR) CSCI	
160	Computer Operator: Initialize a ADSVR CSCI , establish an Admin. session, select the Advertising DB schema update function, and configure the ADSVR schema update function to monitor the status of the session.	
170	Expected results: The selected ADSVR CSCI is available, an Admin./Ops session is established, the Advertising DB schemata update function provides a default screen for viewing Advertising DB schema information, and there are no errors resulting from the session establishment.	
180	Computer Operator: Select an Advertising DB collection and a schema within that collection to update.	
190	Expected Results: Session remains established, Computer Operator does not select a new display to " View" the schemata, no status error from selection actions is presented and the Schema is returned and displayed for update.	
200	Computer Operator: Monitor the Update status indicators and performs the data entry to update the schema.	
210	Expected Results: Session remains established, Computer Operator does not select a new display to "View" the schemata, no errors from the Schema update actions are presented and the Schema remains displayed while Computer Operator reviews his/her update inputs.	
220	Computer Operator: Monitor the Update service status indicators, request status of the schema update be provided by the service, and submit the schemata update to the ADSVR.	
230	Expected Results: Session remains established, Computer Operator does not select a new display to "View" the schemata, no errors from the submit actions are presented in status messages.	
240	Computer Operator: Monitor service status indicators and request status of the schema update submit be provided by the Advertising DB Schema Update service.	
250	Expected Results: Session remains established, Computer Operator does not select a new display to "View" the schema, status message(s) indicate that selected Advertising DB collection schema has been accepted and updated, no errors from the accept and update actions are presented in status messages, "new" Advertising DB collection schema is presented without having to change the update service "view" screen(s). Schema contains all update entered by the tester	
260	Computer Operator: Monitor service status indicators for schema update activities and request ADSRV Admin. service to terminate both the Advertising DB Schema update and Admin. service sessions.	
270	Expected Results: Sessions are terminated without error messages, no status messages about updated schema are presented, and no error status messages about session termination are presented.	

	Data Dictionary (DDICT) CSCI	
300	Computer Operator: Initialize a DDICT CSCI , establishes an Admin. session, selects the dictionary DB schema update function, and configures the DDICT schema update function to monitor the status of the session.	
305	Expected results: The selected DDICT CSCI is available, an Admin./Ops session is established, the dictionary DB schemata update function provides a default screen for viewing DB schema information, and there are no errors resulting from the session establishment.	
310	Computer Operator: Select a dictionary DB collection and a schema within that collection to update.	
315	Expected Results: Session remains established, Computer Operator does not select a new display to "View" the schemata, no status error from selection actions is presented and the Schema is returned and displayed for update.	
320	Computer Operator: Monitor the Schema Update status indicators and perform the data entry to update the schema.	
325	Expected Results: Session remains established, Computer Operator does not select a new display to "View" the schemata, no errors from update actions are presented, and the Schema remains displayed while Computer Operator reviews his/her update inputs.	
330	Computer Operator: Monitors service status indicators, request status of the schema update activities be provided by the service, and submit the schemata update to the dictionary DB.	
335	Expected Results: Session remains established, Computer Operator does not select a new display to "View" the schemata, no errors from the submit actions are presented in status messages.	
340	Computer Operator: Monitor the schema Update service status indicators and request status of the schema update submit be provided by the DDICT DB Update service.	
345	Expected Results: Session remains established, Computer Operator does not select a new display to "View" the schema, status message(s) indicate that selected Dictionary DB collection schema has been accepted and updated, no errors from the accept and update actions are presented in status messages, "new" DB collection schema is presented without having to change the update service "view" screen(s). Schema contains all updates entered by the tester	
350	Computer Operator: Monitor service status indicators for schema update activities and request DDICT Admin. service to terminate both the Dictionary DB Schema update and Admin. service sessions.	
355	Expected Results: Sessions are terminated without error messages, no status messages about updated schema are presented, and no error status messages about session termination are presented.	

Data Reduction and Analysis Steps:	
Signature:	**Date:**

8.1.6 Site Data/Metadata/Information Management Sequence

The GSFC DAAC is evaluated for its ability to perform file management of ECS data/metadata/application information. The ECS ability to maintain a file directory of the files under its control is also verified.

The GSFC DAAC's ability to produce specified backups is also included in this sequence. The ECS capability for storage of ECS data/metadata information in local and off-site locations is verified.

Configuration: The subsystem needed to perform this sequence of tests are as follows. CSS/MSS, DSS, INS, ISS, & PLS. Refer to Appendix D for additional detail.

External Interfaces: There are no external interfaces needed for this sequence.

Operator Position(s): The operator position from the ECS Maintenance and Operations Position Descriptions document (607/OP2) needed to support this sequence is listed:

DAAC Computer Operator

DAAC System Administrator

Operational Scenario(s): The operations scenario, taken from the Operations Scenarios for the ECS Project: Release-A document (605/OP1), that was used to develop tests in this sequence of tests are listed:

Computer System Administration Backup & Restore/Recovery Scenario (Section 3.1.2)

Test Dependencies: There are no test dependencies needed for this sequence of tests.

8.1.6.1 File Management

TEST Procedure No.: A080170.010$G	**Date Executed:**	**Test Conductor:**
Title: File Management		
Objective: The purpose of the test is to confirm the site's capability to perform File Directory Management functions. The AT team confirms by demonstration, that mechanisms are included in the system for File Directory Management functions.		

Requirements	Acceptance Criteria
DADS1530#A	This requirement is verified through demonstration. Each DADS shall maintain a File Directory of all data files which have been archived and are under its control. The Tester verifies that a File Directory of archived data files exists.

DADS1550#A	This requirement is verified through demonstration. Operations/systems personnel shall be able to access, list, or modify the contents of the file directory in a special privileged mode. The Tester verifies that the system provides a mechanism to create the File Directory. The Tester verifies that system provides a mechanism to append, display, update, and print records to the File Directory.

Test Inputs:

Data Set Name	Data Set ID	File Name	Description	Version
TEMP_001		Temp1		
TEMP_002		Temp2		

Step-By-Step Procedures		
Step No.	**Input Action / Expected Results**	**Pass / Fail / Comments**
10	System Administrator: Login to the Science Data Server.	
20	Expected Results: The Science Data Server is available.	
30	System Administrator: Display the directory containing the Archive Log Files	
40	Expected Results: The Archive Log file directory list is displayed on the screen.	
50	System Administrator: Display the archive directory.	
60	Expected Results: The Archive Directory list is displayed on the screen.	
70	System Administrator: Open a file, "Temp1," in the Archive Directory.	
80	Expected Results: The system displays the "Temp1" file.	
90	System Administrator: Edits "Temp1" and saves it.	
100	Expected Results: The edited version of "Temp1" is stored.	
110	System Administrator: Creates a file, "Temp2", and saves it in the Archive Directory.	
120	Expected Results: The new file, "Temp2," is stored in the Archive Directory.	
130	System Administrator: Opens "Temp1" and views the edited version of the file.	
140	Expected Results: The edited version is displayed on the screen.	
160	System Administrator: Opens "Temp2" and views the edited version of the file.	
170	Expected Results: The new file, "Temp2," is displayed on the screen.	
	System Administrator: Appends data to "Temp1."	
	Expected Result: Data is appended to "Temp1."	
	System Administrator: Opens "Temp1."	
	Expected Result: "Temp1" is displayed on the screen containing the original information and the appended data.	
	System Administrator: Prints "Temp1" and "Temp2."	
	Expected Results: A hardcopy of "Temp1" and "Temp2" are produced by the printer.	
	System Administrator: Examines the hardcopy of "Temp1" and "Temp2" comparing it to the information displayed on the screen.	
	Expected Results: The comparison of "Temp1" and "Temp2" verifies the contents of the files.	

Data Reduction and Analysis Steps:	
a. The following are secured for analysis at the close of the procedure: 1. Archive logs. 2. Hardcopies of the files.	
Signature:	**Date:**

8.1.6.2 ECS Storage/Archive/Backup Capability

TEST Procedure No.: A080170.020$G	**Date Executed:**	**Test Conductor:**
Title: ECS Storage/Archive/Backup Capability		
Objective: The purpose of the test is to confirm the site's capability to store, archive, and backup data.		

Requirements	Acceptance Criteria
DADS0425#A	This requirement is verified through inspection. Archive and backup media at each DADS shall have a rated shelf life of at least 10 years as determined by the National Archives and Records Administration (NARA), National Institute for Standards and Technology (NIST), NASA, or a professional or industry organization such as ANSI, the Society of Motion Picture and Television Engineers (SMPTE) or the National Association of Broadcasters (NAB). The tester reviews the backup media's specs and verifies that the manufactured shelf life of the backup media is of at least 10 years when stored in a controlled environment. **Change verification method from test to inspection.**
DADS0430#A	This requirement is verified through test. Each DADS shall provide its operations personnel the capability to manually alter the routing of data sets to physical storage locations. The Tester verifies that the system provides the capability to display, change, and print the allocation of storage devices to Data Servers.
DADS0435#A	This requirement is verified through test. At each DADS operations personnel shall be able to add new physical volumes and eject physical volumes from the archive for off-line or off-site permanent storage. The Tester verifies the ability to mount, insert into, remove from, and dismount archive media storage devices which support removable media.
DADS1370#A	This requirement is verified through test. Each DADS shall provide a mechanism for statistically monitoring both the raw and corrected bit error rate (BER) of storage media in the archive. The Tester verifies that the system calculates a checksum for each file associated with each data granule stored in the archive. **Need further information on implementation. On ESDIS List.**
DADS1375#A	This requirement is verified through test. Each DADS shall provide automatic management and copying/refresh of archive media. **Need further information on implementation. On ESDIS List.**

DADS1710#A	This requirement is verified through demonstration. The DADS shall comply with evolving guidelines and standards in such areas as file storage, storage management, and backup where appropriate. The System must provide the capability to insert, initialize, load, unload and remove archive media into storage devices which support removable media. The System must provide the capability to perform physical inventories of archive media resident in archive storage devices.
DADS1791#A	This requirement is verified through demonstration. Each DADS shall have the capability to mount archival media via automated means. The Tester mounts archival media using the storage device allocation function of the system.
DADS2270#A	This requirement is verified through demonstration. Each DADS shall provide, on a scheduled basis, an off-site backup copy of all EOS data which would be impossible or difficult to recover in case of loss. The Tester verifies the existence of an off-site backup copy of data.
DADS2300#A	This requirement is verified through demonstration. Each DADS shall provide a capability for local and offsite backup/restore of system files. This test does not verify the restore capabilities of this requirement. The Tester verifies the ability to create local and offsite backups.
DADS2302#A	This requirement is verified through demonstration. Offsite and local backup media shall be based on published, open, and non-proprietary formats which fully describe the physical organization and structure of files. The Tester verifies that the backup archive media conforms to openly published and non-proprietary formats for recording data.
DADS2910#A	This requirement is verified through demonstration. Archival storage at each DADS shall be field-expandable. Field-expandable is defined as increasing the capacity or size of archive storage without removing archive storage device from site. **Need further information on implementation. On ESDIS List.**
DADS3000#A	This requirement is verified through demonstration. To support archival data integrity, the bit error rate after correction shall be less than 1 in 10 to the 12th. **Need further information on implementation. On ESDIS List.**
DADS3010#A	This requirement is verified through inspection. Archival and backup media at each DADS shall have a manufacture-rated shelf life of at least 10 years when stored in a controlled environment. The Tester reviews the backup media's specs and verifies that the manufactured shelf life of the backup media is of at least 10 years when stored in a controlled environment.
DADS3040#A	This requirement is verified through test. At each DADS backup media shall be removable from the DADS site (e.g., for safe off-site storage). The Tester verifies the existence of an off-site backup copy of data.

DADS3055#A	This requirement is verified through test. At each DADS all backup media shall be capable of being mounted automatically where appropriate, with the provision for manual failover. The Tester verifies that the system provides the capability mount on-line backup media via automated means.
EOSD3200#A	This requirement is verified through test. A minimum of one backup which is maintained in a separate physical location shall be maintained for ECS software and key data items. The Tester verifies the existence of an off-site backup copy of data.
EOSD3220#A	This requirement is verified through inspection. All media shall be handled and stored in protected areas with environmental and accounting procedures applied. The Tester verifies the existence of an off-site backup copy of data and verify the environmental and accounting procedures are applied in accordance with the Property Management Plan for the ECS Project (602/OP1).

Test Inputs: Mission Operation Procedures for the ECS Project (611/OP3)
Property Management Plan for the ECS Project (602/OP1)

Data Set Name	Data Set ID	File Name	Description	Version
NMC_001			NMC data	
VIRS_001			VIRS 1A, 1B, algorithms	
VIRS_002			VIRS Browse data	

Step-By-Step Procedures		
Step No.	**Input Action / Expected Results**	**Pass / Fail / Comments**
10	Computer Operator: Insert the backup media into the storage device. Initialize storage device.	
20	Expected Results: Storage device is initialized.	
30	Computer Operator: Obtain backup media specs. Using the backup media's specs, verify that the manufactured shelf life of the backup media is of at least 10 years when stored in a controlled environment.	
40	Expected Results: The backup media's specs state that the manufactured shelf life of the media is at least 10 years.	
50	Computer Operator: Load and view contents of backup media.	
60	Expected Results: Backup media blank.	
70	Computer Operator: Accesses storage device allocation screen.	
80	Expected Results: Storage device allocation screen appears.	
90	Computer Operator: Allocates storage devices for backup.	
100	Expected Results: Storage device allocation screen depicts desired allocations.	
110	Computer Operator: Execute Autosys backup software. Initiate complete system backup.	
120	Expected Results: Backup software executes system backup. Backup completes.	
130	Computer Operator: Lists files contained on the backup media. Verifies content of the listing.	
140	Expected Results: Displays files contained on the backup media.	
150	Computer Operator: Dumps contents of the backup media. Verifies the format of the data.	
160	Expected Results: The backup media must be based on published, open, and non-proprietary formats which fully describe the physical organization and structure of files.	
170	Computer Operator: Invokes the word processor to review the QA report on the backup job.	
180	Expected Results: The QA report displays on the screen. The QA report must contain a file listing with the last update date and time and a tapescan with a dump of the first and last file.	
190	Computer Operator: Opens the log file. Updates the backup log with an entry indicating the status of the backup. Saves updated backup log.	
200	Expected Results: The log file displays on the terminal. The updated log file is stored.	

210	Computer Operator: Insert the backup copy media into another storage device. Initialize this storage device.	
220	Expected Results: Storage device is initialized.	
230	Computer Operator: Makes a copy of the backup.	
240	Expected Results: The software performs the copy. Copy completes.	
250	Computer Operator: Unload and remove backup media from the storage devices.	
260	Computer Operator: Marks the copy for off-site storage. Store backup in protected area. Store backup copy in an off-site protected area.	
270	Expected Results: Backup copy is marked and stored in an off-site protected area in accordance with the Property Management Plan for the ECS Project (602/OP1). Backup is stored locally in a protected area in accordance with the Property Management Plan for the ECS Project (602/OP1).	
280	Computer Operator: Generates a QA report on the copied media. Reviews the QA report on the copied media.	
290	Expected Results: The Copied media QA report displays on the screen. The QA report must contain a file listing with the last update date and time and a tapescan with a dump of the first and last file.	
300	Computer Operator: Updates the backup log with an entry indicating the status of the copy of the backup. Saves updated backup log.	
310	Expected Operator: The log file displays on the terminal. The updated log file is stored.	
Data Reduction and Analysis Steps: a. Verify the accounting procedures for handling the backup media is in accordance with the Property Management Plan for the ECS Project (602/OP1).		
Signature:		**Date:**

8.1.7 Facilities Interfaces Sequence

This sequence verifies the basic connectivity and fundamental protocols for GSFC ECS DAAC external and internal interfaces in support of Release A operations. Confirmation of ECS internal (SMC, EOC, LaRC, and EDC) and external interfaces (TSDIS and V0 DAACs) is performed through inspection of before and after data transmission products compared to requirements. Internal ECS interfaces are evaluated similarly. The operational version of external systems are used if they are mature and available at the time of acceptance testing on this sequence. Otherwise, simulators are used.

Configuration: The subsystem needed to perform this sequence of tests are as follows. CSS/MSS, DSS, INS, ISS, & PLS. Refer to Appendix D for additional detail.

External Interfaces: The external interfaces (i.e. other ECS sites and data sources) needed for this sequence (both real and simulated) are listed:

TSDIS Simulator

SMC

EOC

LaRC ECS DAAC

EDC ECS DAAC

GSFC V0 DAAC

LaRC V0 DAAC

EDC V0 DAAC

MSFC V0 DAAC

NOAA ADC

Operator Position(s): The operator positions from the ECS Maintenance and Operations Position Descriptions document (607/OP2) needed to support this sequence are listed:

DAAC Computer Operator

SMCC Computer Operator

Operational Scenario(s): There are no operations scenarios, taken from the Operations Scenarios for the ECS Project: Release-A (605/OP1), used during this sequence of tests.

Test Dependencies: The following table identifies the test procedure(s) in a sequence of tests that should be run prior to or concurrently with a sequence or test procedure.

Test Procedure No.	Site/Procedure No.	Comments
A080180.090$G	A080180.090$L A080180.090$E A080180.090$F A080180.090$S	Concurrent

8.1.7.1 SMC External Interfaces

This test procedure is not applicable for the GSFC Volume of the Acceptance Test Procedures document for Release A.

8.1.7.2 EOC External Interfaces

This test procedure is not applicable for the GSFC Volume of the Acceptance Test Procedures document for Release A.

8.1.7.3 GSFC DAAC External Interfaces

TEST Procedure No.: A080180.050$G	**Date Executed:**	**Test Conductor:**
Title: GSFC DAAC External Interfaces		
Objective: This test case verifies GSFC ECS DAAC connectivity with ECS external systems using the File Transfer Protocol.		

Requirements	Acceptance Criteria
ESN-0070#A	This requirement is verified through test. The ESN shall support the intrasite elements data flow requirements identified in this specification. The ISS must provide for connectivity with external interfaces in order to transfer data to the GSFC ECS DAAC.
ESN-0280#A	This requirement is verified through test. The ESN shall provide file transfer and management service and as a minimum must include the capability to transfer the following data types: a. Unstructured Text b. Binary Unstructured c. Binary Sequential d. Sequential Text The CSS File Access Service must be able to transfer text and binary files.
ESN-0290#A	This requirement is verified through test. The file transfer and management service shall be available in interactive and non-interactive services. The CSS File Access Service must provide functionality for interactive and non-interactive transfer of files (send and receive) between two host systems.
ESN-0300#A	This requirement is verified through test. The file transfer and management non-interactive services shall be able to be scheduled. The CSS File Access Service must provide an option for scheduling file transfers in a batch mode.
IMS-0860#A	This requirement is verified through demonstration. The IMS shall provide an interface to ADC and ODC data systems and archives that produce, process, and/or maintain Earth science data sets and that have agreed to make the information and services available to ECS. The system must be able to transfer data between GSFC and ADC. There are no ODCs in Release A.
IMS-1600#A	This requirement is verified through demonstration. The IMS shall provide access to the following communication services at a minimum: a. File transfer b. Multi media mail c. Remote log-on d. Electronic Bulletin Board e. Access to other networks The system must provided the capability to exchange data via file

	transfer. This test does NOT verify parts b, c, d, or e of the requirement.
NOAA0600#A	This requirement is verified through demonstration. The SAAs shall have the capability to send and the ECS must have the capability to receive Network Management information. The MSS must interface with the Affiliated Data Centers (ADC) to exchange data. **Add verification method to RTM in CCR.**
NOAA0610#A	This requirement is verified through demonstration. The ECS shall have the capability to send and the SAAs must have the capability to receive Network Management information. The MSS must interface with the Affiliated Data Centers (ADC) to exchange data. **Add verification method to RTM in CCR.**
TRMM3120#A	This requirement is verified through test. Communications between TSDIS and the ECS systems at the MSFC DAAC to transport the PR, TMI, and GV standard products, metadata, SSM/I ancillary data, algorithms, and documentation shall be provided by ESDIS. The CSS File Access Service must provide functionality for interactive and non-interactive transfer of files (send and receive) between two host systems. The CSS File Access Service must support the File Transfer Protocol (FTP).
TRMM4110#A	This requirement is verified through test. Communications between TSDIS and the ECS systems at the GSFC ECS DAAC to transport the VIRS standard products, metadata, GPI, GPCP, and NMC ancillary data, and algorithms and documentation shall be provided by ESDIS. The CSS File Access Service must provide functionality for interactive and non-interactive transfer of files (send and receive) between two host systems. The CSS File Access Service must support the File Transfer Protocol (FTP).

Test Inputs:

Data Set Name	Data Set ID	File Name	Description	Version
VIRS_001			VIRS data	
DUMV0_001			Dummy text files from the V0 DAACs	
DUMNOAA_001			Dummy info file from the NOAA ADC	

Step-By-Step Procedures		
Step No.	**Input Action / Expected Results**	**Pass / Fail / Comments**
10	Tester: Set up the TSDIS simulator for transfer of VIRS data.	
20	Expected Results: The TSDIS simulator is on and ready for transfer.	
30	Computer Operator: Access Communications Server and invoke the FTP Software.	
40	Expected Results: FTP software windows displays on the screen.	
50	Computer Operator: Specify binary VIRS file to be transferred. Specify the TSDIS address as the source address and the GSFC address as the destination address for the transfer. Execute transfer.	
60	Expected Results: Transfer complete.	
70	Computer Operator: Verify transmission using system logs and data storage facilities.	
80	Expected Results: System logs contain evidence of the transfer.	
90	Tester: Power down the TSDIS simulator.	
100	Computer Operator: Access FTP Software Window.	
110	Expected Results: FTP software windows becomes active.	
120	Computer Operator: Specify GSFC V0 DAAC text file to be transferred. Specify the GSFC V0 DAAC address as the source address and the GSFC address as the destination address for the transfer. Execute transfer.	
130	Expected Results: Transfer complete.	
140	Computer Operator: Verify transmission using system logs and data storage facilities.	
150	Expected Results: System logs contain evidence of the transfer.	
160	Computer Operator: Access the FTP Software Window.	
170	Expected Results: FTP software window becomes active.	
180	Computer Operator: Specify LaRC V0 DAAC text file to be transferred. Specify the LaRC V0 DAAC address as the source address and the GSFC address as the destination address for the transfer. Execute transfer.	
190	Expected Results: Transfer complete.	
200	Computer Operator: Verify transmission using system logs and data storage facilities.	
210	Expected Results: System logs contain evidence of the transfer.	
220	Computer Operator: Access the FTP Software Window.	
230	Expected Results: FTP software window becomes active.	

240	Computer Operator: Specify MSFC V0 DAAC text file to be transferred. Specify the MSFC V0 DAAC address as the source address and the GSFC address as the destination address for the transfer. Execute transfer.	
250	Expected Results: Transfer complete.	
260	Computer Operator: Verify transmission using system logs and data storage facilities.	
270	Expected Results: System logs contain evidence of the transfer.	
280	Computer Operator: Access the FTP Software Window.	
290	Expected Results: FTP software window becomes active.	
300	Computer Operator: Specify EDC V0 DAAC text file to be transferred. Specify the EDC V0 DAAC address as the source address and the GSFC address as the destination address for the transfer. Execute transfer.	
310	Expected Results: Transfer complete.	
320	Computer Operator: Verify transmission using system logs and data storage facilities.	
330	Expected Results: System logs contain evidence of the transfer.	
340	Computer Operator: Access the FTP Software Window.	
350	Expected Results: FTP software window becomes active.	
360	Computer Operator: Specify NOAA ADC text file to be transferred. Specify the NOAA ADC address as the source address and the GSFC address as the destination address for the transfer. Execute transfer.	
370	Expected Results: Transfer complete.	
380	Computer Operator: Verify transmission using system logs and data storage facilities.	
390	Expected Results: System logs contain evidence of the transfer.	
400	Computer Operator: Access the FTP Software Window.	
410	Expected Results: FTP software window becomes active.	
420	Computer Operator: Specify GSFC text file to be transferred. Specify the GSFC address as the source address and the NOAA ADC address as the destination address for the transfer. Execute transfer.	
430	Expected Results: Transfer complete.	
440	Computer Operator: Verify transmission using system logs and data storage facilities.	
450	Expected Results: System logs contain evidence of the transfer.	
Data Reduction and Analysis Steps: a. The following are secured for analysis at the close of the procedure: System FTP logs.		
Signature:		**Date:**

8.1.7.4 LaRC DAAC External Interfaces

This test procedure is not applicable for the GSFC Volume of the Acceptance Test Procedures document for Release A.

8.1.7.5 EDC DAAC External Interfaces

This test procedure is not applicable for the GSFC Volume of the Acceptance Test Procedures document for Release A.

8.1.7.6 ECS Internal Interfaces

TEST Procedure No.: A080180.090$G	**Date Executed:**	**Test Conductor:**
Title: ECS Internal Interfaces		
Objective: This test case verifies the capability for the GSFC DAAC to communicate with the LaRC, EDC, SMC and EOC.		

Requirements	Acceptance Criteria
ESN-0010#A	This requirement is verified through test. ESN shall provide the following standard services: a. Data Transfer and Management Services b. Electronic Messaging Service c. Remote Terminal Service d. Process to Process Communication Service e. Directory and User Access Control Service f. Network Management Service g. Network Security and Access Control Service h. Internetwork Interface Services i. Bulletin Board Service The CSS Electronic Mail Service must allow the users to create, modify and delete messages. The CSS Electronic Mail Service must provide the ability to send and receive messages. The CSS Electronic Mail Service must provide the ability to attach files to messages. This test does NOT verify parts c, e, f and g of the requirement.
ESN-0340#A	This requirement is verified through test. The ESN shall interoperate and exchange messages and data with external SMTP and X.400 mail systems. The Tester must verify the ability to provide translation between SMTP and X.400 protocols by creating a message in one protocol and sending/receiving it in another.
ESN-0345#A	This requirement is verified through test. The ESN shall be capable of transparently transmitting Multi-purpose Internet Mail Extensions (MIME) messages. The CSS Electronic Mail Service must be capable of sending and receiving the Multi-purpose Internet Mail Extensions (MIME) messages.
ESN-0350#A	This requirement is verified through test. The Electronic Messaging Service shall be capable of exchanging binary data. The CSS Electronic Mail Service must allow attaching either text or

	binary files to a message.
ESN-0450#A	This requirement is verified through test. The ESN shall provide process-to-process communication service. The CSS Message service must provide an API for senders to send messages to receivers asynchronously without waiting for the receivers to receive it.
ESN-1170#A	This requirement is verified through test. The ESN must provide necessary translation within supported file transfer and e-mail services. The CSS Electronic Mail Service must provide translation between SMTP and X.400 protocol.
ESN-1181#A	This requirement is verified through demonstration. The ESN shall provide an ECS Bulletin Board capability. The CSS Bulletin Board Service must allow the users to post messages to and delete messages from bulletin board(s). The CSS Bulletin Board Service must provide the capability for copying files. The CSS Bulletin Board Service must support multiple bulletin boards. The CSS Bulletin Board Service must allow multiple messages for each bulletin board.
ESN-1350#A	This requirement is verified through inspection. The ESN LANs shall provide physical devices and the corresponding medium access control (MAC) protocol compatible with ISO and ANSI standards. The Tester reviews the physical devices' specs and verifies that the medium access control (MAC) protocol is compatible with ISO and ANSI standards. **Change verification method from analysis to inspection.**
IMS-1600#A	This requirement is verified through demonstration. The IMS shall provide access to the following communication services at a minimum: a. File transfer b. Multi media mail c. Remote log-on d. Electronic Bulletin Board e. Access to other networks The Tester verifies the capabilities of the CSS Mail Service and the CSS Bulletin Board Service. This test does not verify parts a, c and e of the requirement.
NSI-0010#A	This requirement is verified through test. NSI, responsible for EOSDIS "Mission Success" network services, shall provide network connectivity to the following ECS facilities: a._ECS at the GSFC DAAC, Goddard Space Flight Center (GSFC), Greenbelt, Maryland c._System Monitoring and Coordination facility (SMC), Goddard Space Flight Center (GSFC), Greenbelt, Maryland f._ECS at the LaRC DAAC, Langley Research Center (LaRC), Hampton, Virginia The GSFC DAAC must be able to transfer data with the SMC and LaRC DAAC.
SMC-2120#A	This requirement is verified through demonstration. The SMC shall make available for automated distribution to authorized users all unlicensed toolkit software, toolkit software upgrades, and toolkit documentation.

	The GSFC DAAC LSM must be able to access authorized unlicensed toolkit software, toolkit software upgrades, and toolkit documentation via the bulletin board.
SMC-2610#A	This requirement is verified through demonstration. The SMC shall provide and maintain a bulletin board service with information on ECS status, events, and news. The GSFC DAAC LSM must be able to obtain information on ECS status, events, and news via the bulletin board.

Test Inputs: Valid account names and passwords for accounts at each DAAC, SMC and EOC.

Data Set Name	Data Set ID	File Name	Description	Version
TOOLKIT_001			authorized unlicensed toolkit software	
TOOLKIT_002			toolkit software upgrades	
TOOLKIT_003			toolkit documentation	
EMAIL_001			Sample E-mail message	
EMAIL_002			Sample E-mail attachment	

Step-By-Step Procedures		
Step No.	**Input Action / Expected Results**	**Pass / Fail / Comments**
10	Computer Operator: Access Communications Server and invoke E-mail client.	
20	Computer Operator: Create a new message. Specify E-mail address at LaRC DAAC. Specify subject and body of message to be sent to LaRC DAAC. Attach file to the message. Send the message to LaRC DAAC.	
30	Computer Operator: Select message sent to LaRC. Change E-mail address at EDC DAAC. Edit subject and body of message to be sent to EDC DAAC. Attach file to the message. Send the message to EDC DAAC.	
40	Computer Operator: Create a new message. Specify E-mail address at SMC. Specify subject and body of message to be sent to SMC. Attach text and binary files to the message. Send the message to SMC.	
50	Computer Operator: Create a new message. Specify E-mail address at EOC. Specify subject and body of message to be sent to EOC. Attach file to the message. Send the message to EOC.	
60	Computer Operator: View GSFC E-mail logs to verify transmission of each E-mail message.	
70	Expected Results: System logs reflect transmission of each E-mail message.	
80	LaRC Computer Operator: Views E-mail. The message is inspected for evidence of transmission errors.	
90	Expected Results: The message transmission does not contain any evidence of transmission errors, such as garbled text.	
100	LaRC Computer Operator: Creates a reply message specifying E-mail address at GSFC DAAC as well as the subject and body of message. Send the message to GSFC DAAC.	
110	Computer Operator: Opens reply message verifying receipt of reply message. Print and delete message.	
120	Expected Results: The hardcopy is available from the printer. The message no longer resides in the In box.	
130	EDC Computer Operator: Views E-mail. The message is inspected for evidence of transmission errors.	
140	Expected Results: The message transmission does not contain any evidence of transmission errors, such as garbled text.	
150	EDC Computer Operator: Creates a reply message specifying E-mail address at GSFC DAAC as well as the subject and body of message. Send the message to GSFC DAAC.	
160	Computer Operator: Opens reply message verifying receipt of reply message. Print and delete message.	

170	Expected Results: The hardcopy is available from the printer. The message no longer resides in the In box.	
180	SMC Computer Operator: Views E-mail. The message is inspected for evidence of transmission errors.	
190	Expected Results: The message transmission does not contain any evidence of transmission errors, such as garbled text.	
200	SMC Computer Operator: Creates a reply message specifying E-mail address at GSFC DAAC as well as the subject and body of message. Send the message to GSFC DAAC.	
210	Computer Operator: Opens reply message verifying receipt of reply message. Print and delete message.	
220	Expected Results: The hardcopy is available from the printer. The message no longer resides in the In box.	
230	EOC Computer Operator: Views E-mail. The message is inspected for evidence of transmission errors.	
240	Expected Results: The message transmission does not contain any evidence of transmission errors, such as garbled text.	
250	EOC Computer Operator: Creates a reply message specifying E-mail address at GSFC DAAC as well as the subject and body of message. Send the message to GSFC DAAC.	
260	Computer Operator: Opens reply message verifying receipt of reply message. Print and delete message.	
270	Expected Results: The hardcopy is available from the printer. The message no longer resides in the In box.	
280	Computer Operator: Creates multiple messages and posts them to a bulletin board.	
290	Computer Operator: Accesses the bulletin board and verifies that the messages are present.	
300	Expected Result: The messages are accessible through the bulletin board.	
310	Computer Operator: Creates multiple messages and posts them to multiple bulletin boards.	
320	Computer Operator: Accesses the bulletin boards and verifies that the messages are present.	
330	Expected Result: The messages are accessible through the bulletin boards.	
340	Computer Operator: Copies authorized unlicensed toolkit software, toolkit software upgrade, and toolkit documentation files from the bulletin board.	
350	Expected Result: Lists the contents of the directory to verify the receipt of the downloaded file.	
360	Computer Operator: Deletes a message from the bulletin board.	
370	Expected Result: The bulletin board refreshes without the deleted message reflecting the deletion.	
380	Computer Operator: Accesses a different bulletin board and deletes multiple messages.	

390	Expected Result: The bulletin board refreshes without the deleted message reflecting the deletion.	
Data Reduction and Analysis Steps:		
Signature:		**Date:**

8.2 Scheduling Scenario

The Scheduling Scenario verifies the ability to generate a series of schedules involving his/her site and support by other sites. It follows the process of scheduling the activities at each site, coordinating them with other sites through the SMC and resolving scheduling conflicts when they arise. The scenario then continues with the development of a coordinated master schedule by SMC operators. It carries the SMC operators through the schedule request, development, confirmation and adjudication process; returning in full-circle to the scheduler who initiated the schedule request.

The purpose of this scenario is to evaluate the ECS site-level scheduling capability. ECS capability for acquiring, storing and maintaining schedules, negotiating and maintaining ground event functional allocations and priorities are assessed. SMC procedures for acquiring and maintaining ECS schedules, and for generating associated site-to-site and site-to-site integration, test, simulation, operations and maintenance directives are also evaluated.

This scenario also evaluates procedures for adjudicating cross-site and cross-facility schedule conflicts in the best interests of the systems users and in a manner that promotes the most efficient use of all ECS site and the total ECS system.

Procedures for receiving and analyzing product generation schedules from the DAACs and other ECS sites are evaluated as well as SMC's methodology for recommending, reviewing, approving and disseminating information related to schedule implementations or adjustments.

Each site's LSM scheduling activity is evaluated for its ability to communicate and receive scheduling information from the SMC as well as its effectiveness in monitoring, coordinating and implementing SMC integrated schedules within assigned sites.

8.2.1 Schedule Generation Sequence

The Schedule Generation Sequence evaluates the schedule generation process as implemented at GSFC. The confirms the ECS systems scheduler's capability for generating, analyzing inputs, integrating, and distributing approved site-level schedules and for developing and communicating appropriate site scheduling guidelines for instrument and ground event scheduling. The receipt, analysis and implementation of scheduling directives by the GSFC LSM and subsequent coordination and implementation by GSFC scheduling personnel into site planning are evaluated.

Configuration: The subsystem needed to perform this sequence of tests are as follows. CSS/MSS, DSS, INS, ISS, & PLS. Refer to Appendix D for additional detail.

External Interfaces: The external interface (i.e. other ECS sites and data sources) needed for this sequence (both real and simulated) is listed:

SMC

Operator Position(s): The operator position from the ECS Maintenance and Operations Position Descriptions document (607/OP2) needed to support this sequence are listed:

DAAC Production Planner

Operational Scenario(s): The operations scenarios, taken from the Operations Scenarios for the ECS Project: Release-A document (605/OP1), that were used to develop tests in this sequence of tests are listed:

Resource Planning Scenario (Section 3.7.1)

Routine Production Planning Scenario (Section 3.12.1)

Test Dependencies: The following table identifies the test procedure(s) for this sequence of tests that should be run prior to or concurrently with this test procedure.

Test Procedure No.	Site/Procedure No.	Comments
A080210.010$G	A080210.010$S	Concurrent
A080210.020$G	A080210.020$S	Concurrent

8.2.1.1 DAAC Schedule Generation

TEST Procedure No.: A080210.010$G	**Date Executed:**	**Test Conductor:**
Title:	DAAC Schedule Generation	
Objective:	The DAAC Schedule Generation test case is designed to test the DAAC's operational capabilities in requesting, accessing and making use of scheduling information received from the SMC. The test starts with a request by the DAAC to be included in an upcoming schedule-related-event. This involves an already distributed SMC schedule. This test case will demonstrate that the DAAC has capabilities to receive and accept schedule directives from the SMC, verify access to system-wide scheduling information provided, and convey non-instrument related schedules for ground operations within the DAAC and other ECS sites.	

Requirements	Acceptance Criteria
DADS1980#A	This requirement is verified through demonstration. Each DADS shall receive from the SMC scheduling directives for system level, site/element-to-site/element, testing, and simulation activities. The GSFC DAAC must be able to receive scheduling directives from the SMC.
DADS2110#A	This requirement is verified through demonstration. The DADS shall provide scheduling information to the SMC. The DADS must make scheduling information available to the SMC.
DADS2120#A	This requirement is verified through demonstration.

	The DADS shall have access to the system wide scheduling information. Such information includes, at a minimum, ESDIS Policies and Procedures regarding instrument and ground event scheduling, other element plans and schedules, element allocations of ground event functions and capabilities, product thread information, and scheduling directives for testing, maintenance, and emergency situations. The GSFC DAAC must be able to access system wide scheduling information.
DADS2210#A	This requirement is verified through demonstration. Each DADS shall provide tools for the creation and manipulation of its plans/schedules. Tools for scheduling must be present at GSFC. During the test, these tools must be used to create daily, 10 day and 30 day schedules.
Test Inputs: SMC schedule directive	

Step-By-Step Procedures		
Step No.	**Input Action / Expected Results**	**Pass / Fail / Comments**
10	Production Planner: Reviews objectives for processing for the coming month. Considerations are: - SS Stability, - IT input, and - Project directives. Notes that the current PR for a MODIS product is due to expire. The IT for a MODIS has requested that the PR be reissued for the next month.	
20	Expected Result: E-mail from Its to operations is supported. Depending on local DAAC policy, the lead SCF may also access production request editor directly to enter production requests.	
30	Production Planner: Starts the production request editor from the normal operators desktop.	
40	Expected Result: The production request editor displays on the screen.	
50	Production Planner: Selects the option to access the existing PRs. A window is open that provides the collection of fields that constitute a PR.	
60	Expected Results: The production request editor provides several fields to be input by the user.	
70	Production Planner: In the “Instrument” field, the planner selects MODIS from a list of options. From the “Processing Level/Description” field, the planner selects “ERBE-like” processing. From the ”PGE” field,the planner selects the PGE ID that is the most current for the ERBE-like processing, which is the default. Scrolls through the list of user parameters and corresponding values, but makes no changes. Scrolls through a list of paired start/stop dates for processing that have been previously entered for this configuration of times and user parameters. Enters in a new pare of start/stop date values corresponding to the monthly period requested by the MODIS IT. Clicks ‘Add PR’ and exits the production request editor window.	

80	Expected Results: The system uses the production request to generate a series of data processing requests. Each DPR corresponds to the execution of a single PGE. At this point, the availability of the data required for each DPR is checked, either from the data server if the data are previously ingested, or from internal predictions if the data are expected to arrive in the future. Also, at this point, the data to be output from the DPR are calculated to generate predictions of what may be available for subsequent PGEs.	
90	Production Planner: Creates a plan for the coming month. Starts the planning workbench.	
100	Expected Result: The planning workbench is started from the normal operators desktop	
110	Production Planner: Selects the New Plan option.	
120	Expected Results: The planning workbench displays the options available.	
130	Production Planner: Indicates the time period (start/stop dates) for which he wishes to develop a plan.	
140	Expected Results: The planning workbench is configurable for each DAAC to suit their needs. The planning workbench displays PRs that are applicable to the specified planning interval. Each PR is identified by a row in the list which contains information such as the PR name, PGE ID, priority, time period, comments and whether the PR has been scheduled for this plan.	
150	Production Planner: The planner is uncertain concerning the details of one of the PRs displayed and selects to view the details for the PR instead.	
160	Expected Results: The system displays a detail screen for a single PR, identifying all of the information describing the job.	
170	Production Planner: Reverts to the PR scrollable list display and selects all of the PRs applicable to this period.	
180	Expected Results: The list of all possible PRs are selected for inclusion in the planning activity. Viewing the PRs either via the PR detail GUI or the PR scrolling list, the operator can select or deselect individual PRs and change their priority or toggle them to be scheduled or unscheduled.	
190	Production Planner: After selecting the PRs to be run during the planning interval, Selects “Schedule” to indicate completion of PR selection.	
200	Production Planner: Clicks on “Timeline” which creates a plan from the selected PRs and presents it as a timeline display.	
210	Expect Results: The system uses the selected PRs, information concerning the projected run time of the jobs, system resource projections including ground event activities, and priorities associated with jobs to develop a monthly plan.	

220	Production Planner: Considers the resulting plan. Notes that not all the intended processing objectives are accomplished. This is the result of the large amount of ground event time allocated to production resources during this interval to meet certain test objectives. Decides to develop a second candidate plan where the priority of some reprocessing activities are lowered t allow standard processing objectives to be met. The planner is aware that the testing activities will be completed shortly after and that sufficient resources will be available to keep current with standard processing and work off the backlog of reprocessing. Exits from the plan viewing GUI, saves the current plan, and returns to the plan creation activity.	
230	Expected Results: The plan creation activity is displayed on the screen.	
240	Production Planner: Reviews the list of PRs selected previously. Selects a PR corresponding to a reprocessing activity.	
250	Expected Results: The reprocessing activity PR is displayed.	
260	Production Planner: Modifies the priority level for the PR for the time period and selects "Schedule" to indicate completion of PR modification.	
270	Expected Results: The planning system can save multiple plans during a session that can be retrieved later in the session. The priority can be changed from the PR Id list GUI.	
280	Production Planner: Clicks on "Timeline".	
290	Expected Results: The planning system can save multiple plans during a session that can be retrieved later in the session. The priority can be changed from the PR Id list GUI.	
300	Production Planner: Considers the second candidate plan created. The expected result of the priority change is achieved. The planner saves this monthly production plan.	
310	Expected Results: The planning system can save multiple plans during a session that can be retrieved later in the session. The priority can be changed from the PR Id list GUI.	
320	Production Planner: Exits from the plan creation GUIs.	
330	Expected Results: The planning workbench is displayed.	
340	Production Planner: Selects "Baseline Plan" to establish a point of comparison to be used for "Planned vs. Actuals" comparisons.	
350	Expected Results: The planning workbench creates a tabular presentation of the information contained in the plan and transfers the resulting document to the Document Data Server (DDS) where it will be available to the public. (A graphical version of this plan accessible via the DDS is TBD).	

360	Production Planner: Creates a Weekly Plan for the coming week. The underlying information in the planning system data base is the same for both the monthly plan and the Weekly Plan, but reports generated provide more detailed information. Selects the "Open" option to open an existing plan for the week.	
370	Expected Results: The planning workbench displays the options available.	
380	Production Planner: Reviews and updates the selected PRs where required reflecting planning meetings and comments.	
390	Expected Results: The planning workbench displays the options available.	
400	Production Planner: Clicks on "Timeline" to view the resulting plan for the time period. The planner considers the plan created. The expected result of the priority change is achieved.	
410	Expected Results: The planning workbench displays the timeline.	
420	Production Planner: Saves the this monthly plan.	
430	Expected Results: The planning workbench displays the options available.	
440	Production Planner: Exits from the plan creation GUIs.	
450	Expected Results: The planning workbench is displayed.	
460	Production Planner: Selects "Baseline Plan" to establish a point of comparison to be used for "Planned vs. Actuals" comparisons for the weekly plan.	
470	Expected Results: The planning workbench creates a tabular presentation of the information contained in the plan and transfers the resulting document to the Document Data Server (DDS) where it will be available to the public. (A graphical version of this plan accessible via the DDS is TBD).	
480	Production Planner: Reviews the production schedule for the next day of processing. Then, selects the current weekly plan being used for the activation/schedule seeding operation to activate the schedule.	
490	Expected Results: Information from this most current weekly plan will be rolled into the processing system COTS scheduler. The planning workbench options are displayed.	
500	Production Planner: Selects "Activate Plan" from the planning workbench options.	
510	Expected Results: The plan for the day is updated to reflect any changes in the PDPS Planning database such as the status of DPRs that were previously activated for processing, or changes in the resource allocation timeline for processing.	
520	Production Planner: Enters the time range of the scheduling period, and any comments appropriate to the schedule and selects Activate.	

530	Expected Results: The system creates an ordered list of the activities which are currently active in data processing and integrates with it other activities that may be scheduled within the scheduling window or time period. The planning system processes the list: if the DPR is already active (i.e., in the data processing system), the entry available to the data processing system is updated to insure the most current information with possible priority adjustments. If the DPR is not active, it is scheduled into the data processing system.	
540	Production Planner: Reviews the resulting schedule and accepts the results.	
550	Expected Results: The system returns to the Planning Workbench. The data processing system will initiate PGE jobs according to the schedule of jobs transferred from the planning system.	
Data Reduction and Analysis Steps:		
Signature:		**Date:**

8.2.1.2 SMC Schedule Generation

This test procedure is not applicable for the GSFC Volume of the Acceptance Test Procedures document for Release A.

8.2.2 Schedule Adjudication Sequence

The Schedule Adjudication Sequence primarily involves the SMC, to confirm the process for adjudicating ECS schedules. The ECS systems scheduler's abilities to detect, analyze, adjudicate, distribute decisions; and monitoring actions resulting from schedule conflicts are confirmed. The SMC capability for distributing schedule adjudication results is assessed based on comparison with ECS requirements. Finally, system and site procedures for monitoring ECS and each site's progress and thoroughness in making on-site schedule adjustments based on approved adjudication results are inspected.

Configuration: The subsystem needed to perform this sequence of tests are as follows. CSS/MSS, DSS, INS, ISS, & PLS. Refer to Appendix D for additional detail.

External Interfaces: The external interface (i.e. other ECS sites and data sources) needed for this sequence (both real and simulated) is listed:

SMC

Operator Position(s): The operator positions from the ECS Maintenance and Operations Position Descriptions document (607/OP2) needed to support this sequence are listed:

DAAC Production Planner

DAAC Production Monitor

Operational Scenario(s): The operations scenario, taken from the Operations Scenarios for the ECS Project: Release-A document (607/OP2), that was used to develop tests in this sequence of tests are listed:

Replanning Production Scenario (Section 3.12.2)

Test Dependencies: The following table identifies the test procedure(s) for this sequence of tests that should be run prior to or concurrently with this test procedure.

Test Procedure No.	Site/Procedure No.	Comments
A080220.010$G	A080220.010$S	Concurrent

8.2.2.1 Adjudication of ECS Site Conflicts

TEST Procedure No.: A080220.020$G	**Date Executed:**	**Test Conduct or:**
Title:	Adjudication of ECS Site Conflicts	
Objective:	The Adjudicate ECS Site Conflicts Caused by Failed Subsystem Components test case verifies requirements to perform analysis and conflict resolution in response to schedule or resource contention between DAAC subsystem components. It verifies that conflicts are identified and corrective action initiated for partitions of ECS functions at a DAAC site. For example, an instance of resource or schedule conflict caused by: failed operation of site hardware, delayed access to archived data, improper execution or performance of system software, and improper execution or performance of application (ECS services) level software will result in a notification of resource contention being posted by the LSM.	

Requirements	Acceptance Criteria
DADS2090#A	This requirement is verified through demonstration. Each DADS shall reevaluate its schedule after receiving new orders from the IMS. The ECS scheduler must accept changes and modifications to existing schedules.
DADS2210#A	This requirement is verified through demonstration. Each DADS shall provide tools for the creation and manipulation of its plans/schedules. During this test, planning and scheduling tools must be usable by the operations staff to modify existing schedules
DADS2220#A	This requirement is verified through demonstration. Each DADS shall provide tools for manually overriding any of its schedules with other elements. Manual override tools for schedules must be present at GSFC. During the test, these tools must be used to override schedules.
SMC-1345#A	This requirement is verified through test. The LSM shall perform priority management services to resolve conflicts for ECS resources. The LSM must perform priority management services to resolve conflicts for ECS resources.

Step-By-Step Procedures		
Step No.	**Input Action / Expected Results**	**Pass / Fail / Comments**
10	Production Monitor: Notices (via the AutoSys TimeScape GUI) that the planned for objectives of the shift are not being met. Processing has fallen behind schedule. Anticipating questions when products do not appear at the times planned, suggests to the Production Planner that replanning may be advisable to get new projections.	
20	Production Planner: Concurs and starts the planning workbench.	
30	Expected Results: The planning workbench appears on the screen displaying the available options.	
40	Production Planner: Selects and opens the current weekly plan being used for the activation/schedule seeding operation.	
50	Expected Results: The current weekly plan is displayed.	
60	Production Planner: Reviews the resulting schedule and modifies the priority level for the PR for the time period and selects "Schedule" to indicate completion of PR modification.	
70	Expected Results: The planning system saves the plans.	
80	Production Planner: Clicks on "Timeline" to view the resulting plan for the time period. The planner considers the plan created	
90	Expected Results: The planning workbench displays the timeline.	
100	Production Planner: Exits from the plan creation GUIs.	
110	Expected Results: The planning workbench is displayed.	
120	Production Planner: Selects "Baseline Plan" to establish a point of comparison to be used for "Planned vs. Actuals" comparisons.	
130	Expected Results: The planning workbench creates a tabular presentation of the information contained in the plan and transfers the resulting document to the Document Data Server (DDS) where it will be available to the public. (A graphical version of this plan accessible via the DDS is TBD).	
140	Production Planner: Selects "Activate Plan" from the planning workbench options.	
150	Expected Results: Information from this updated plan is rolled into the processing system COTS scheduler.	
160	Production Planner: Enters the time range of the scheduling period, enters any comments appropriate to the schedule and selects Activate.	

170	Expected Results: The system creates an ordered list of the activities which are currently active in data processing and integrates with it other activities that may be scheduled within the scheduling window or time period. The system initiates PGE jobs according to the schedule of jobs transferred from the planning system.	
Data Reduction and Analysis Steps:		
Signature:		**Date:**

8.3 ECS Site Upgrade Scenario

This scenario traces the steps taken by the M&O staff in the process of implementing changes to the ECS site environment. It carries the maintenance personnel through established procedures for system upgrades and enhancements.

The purpose of this scenario is to provide confirmation of the SMC's, each site's, and the total system's ability to successfully evolve through installation of minor enhancements and major upgrades. ECS overall and site capability for ascertaining the validity and assessing impacts of requested modifications is inspected.

8.3.1 Enhancements Sequence

This sequence conducts the AT reviewers through ECS site procedures for coordinating site enhancements with the ECS systems level team. ECS site policy and procedures are inspected to evaluate in-site enhancement policies. Analysis is performed to provide evidence that proper coordination actions with SMC takes place that update SMC retained site architecture's procedures to reflect the newly installed enhancement. Site procedures are reviewed for assurance that integrated system-level enhancement related policies and procedures are in force within ECS sites.

LSM procedures for receiving monitoring and reporting on SMC originated site enhancements are assessed. LSM procedures and activities for coordinating with site management and monitoring site implementation team enhancement activities, to confirm appropriate use of integrated toolkits and standard user interfaces are evaluated.

Configuration: The subsystem needed to perform this sequence of tests are as follows. CSS/MSS, DSS, INS, ISS, & PLS. Refer to Appendix D for additional detail.

External Interfaces: The external interfaces (i.e. other ECS sites and data sources) needed for this sequence (both real and simulated) are listed:

SMC

LaRC ECS DAAC

Operator Position(s): The operator positions from the ECS Maintenance and Operations Position Descriptions document (607/OP2) needed to support this sequence are listed:

DAAC User Services Representative

Screening Committee

SMC CM Administrator

SEO

GSFC Site CCB

(includes DAAC Operations Supervisor, DAAC Resource Manager, others TBD)

Operational Scenario(s): The operations scenario, taken from the Operations Scenarios for the ECS Project: Release-A document (605/OP1), that was used to develop tests in this sequence of tests are listed:

System Enhancement Scenario (Section 3.4.7)

Test Dependencies: There are no test dependencies needed for this sequence of tests.

8.3.1.1 ECS Enhancements

TEST Procedure No.: A080320.010$G	**Date Executed:**	**Test Conductor:**
Title:	ECS Enhancements	
Objective:	This test provides ECS software, hardware and general managers with assurance that the GSFC DAAC has satisfactory software enhancement procedures in place. Each applicable written policy, procedures and as-built architecture specifications for managing and performing system enhancements are required inputs for this test case. Procedures are inspected for satisfactory life cycle coverage of enhancement initiation, implementation, and installation. Enhancement configuration management procedures are inspected and compared with enhancement procedures for specification of timely reviews and baseline updates that assure the site's ability to update and retain configuration status.	

Requirements	**Acceptance Criteria**
SMC-2535#A	This requirement is verified through demonstration. Upon approval of an enhancement, the LSM must facilitate the implementation of the approved changes within an elements hardware and software. During the test, LSM must assist in installing the software enhancement from the SMC. **Change verification method from analysis to demonstration.**

Test Inputs:

Data Set Name	**Data Set ID**	**File Name**	**Description**	**Version**
SW_001			S/W enhancement file	
CCR_001			CCR	

Step-By-Step Procedures		
Step No.	**Input Action / Expected Results**	**Pass / Fail / Comments**
10	User Services Representative: Accesses URDB to submit an enhancement recommendation for one of the ECS custom toolkits.	
20	Expected Results: URDB input screen is displayed on the screen.	
30	User Services Representative: Enters his/her name, e-mail address, phone number, agency's name, recommendation title, and the recommendation.	
40	Expected Results: The system provides an ID number for future reference to this recommendation.	
50	Screening Committee: Accesses the URDB.	
60	Expected Results: URDB displays the enhancement recommendation.	
70	Screening Committee: Reviews the enhancement recommendation, determines that the recommendation has merit, has system-wide impact, and should be submitted via a configuration change request (CCR) to ESDIS CCB for approval. Screening Committee Member (SCM): Changes status of recommendation to reflect its consideration for implementation.	
80	Expected Result: URDB stores the status update.	
90	SCM: Executes DDTS to compose the CCR.	
100	Expected Results: The DDTS displays on the screen.	
110	SCM: Clicks the "Submit" button to bring up the CCR input screen.	
120	Expected Results: The DDTS displays the CCR input screen.	
130	SCM: Enters the class and project name for the CCR.	
140	Expected Results: The DDTS accepts the input and displays the CCR form.	
150	SCM: Enters the name of the toolkit, version number, descriptive title for the CCR, recommended priority, recommendation (includes references to the URDB ID number) on the form and then clicks the "Commit" button.	
160	Expected Results: The DDTS stores the CCR information in its data base, sets an initial state (new), and sends e-mail notification of its existence to the SMC CM Administrator and the SEO.	

170	SEO Staff Member (SM): Receives e-mail notification and accesses DDTS.	
180	Expected Results: DDTS displays the CCR.	
190	SM: Reviews the CCR ad prints it to a designated file.	
200	Expected Results: DDTS prints a copy of the CCR to a designated file.	
210	SM: Executes e-mail.	
220	Expected Results: E-mail is displayed on the screen.	
230	SM: Composes a message attaching a copy of the CCR addressed to each site's SE for an impact assessment and sends the message.	
240	Expected Results: E-mail facility transmits the message with the attached CCR file to each site and notifies the recipients that they have mail.	
250	Site SE: Executes e-mail.	
260	Expected Results: E-mail is displayed on the screen.	
270	Site SE: Opens and assesses the message and attached CCR. Creates a forwarded message addressed to the site CM Administrator, the message contains assessment information such as the purpose of the assessment, name of requesting agency, impact to site resources, benefits to site, recommendation, and a copy of the CCR. Sends the message.	
280	Expected Results: E-mail facility transmits the message with the attached CCR file to the Site CM Administrator and notifies the recipient that he/she has mail.	
290	Site CM Administrator: Executes e-mail.	
300	Expected Results: E-mail is displayed on the screen.	
310	Site CM Administrator: Opens and assesses the message and attached CCR and forwards a message addressed to the site CCB for review and approval. Sends the message.	
320	Expected Results: E-mail facility transmits the message with the attached CCR file to the Site CCB and notifies the recipient that he/she has mail.	
330	Site CCB: Executes e-mail.	
340	Expected Results: E-mail is displayed on the screen.	
350	Site CCB: Opens, reviews and approves the assessment.	
360	Site SE: E-mails site assessment to the SEO.	
370	Expected Results: E-mail facility transmits assessment to SEO and notifies the recipient.	

380	SEO SM: Executes e-mail.	
390	Expected Results: E-mail is displayed on the screen.	
400	SEO SM: Opens and reads the sites' assessments.	
410	Expected Result: Assessment appears on the screen.	
420	SEO SM: Accesses DDTS.	
430	Expected Results: DDTS appears on the screen.	
440	SEO SM: Selects the CCR in the index.	
450	Expected Results: The CCR appears on the screen.	
460	SEO SM: Clicks the "Modify" button and then selects the "Add Enclosure" option.	
470	Expected Results: The "Add Enclosure" window appears.	
480	SEO SM: Enters the summary of the impact assessments, cost estimates, and recommendation. Then, executes the editor's File Menu's save option and enters an enclosure title.	
490	Expected Results: DDTS saves the information under the entered enclosure title.	
500	SEO SM: Uses the "Add Enclosure" feature to insert each of the sites' assessment file into an enclosure and names each site's assessment enclosure accordingly.	
510	Expected Results: DDTS saves the content of each file under the entered enclosure title. DDTS sends e-mail notification of the update to the CCR originator, the URDB SCM	
520	SEO SM: Selects the "File" menu then selects "print."	
530	Expected Results: DDTS prints the CCR.	
540	SEO SM: Sends a card copy of the CCR to the ESDIS CCB for review and approval.	
550	ESDIS CCB: Reviews and approves the CCR and issues implementation instructions.	
560	SMC CM Administrator: Accesses URDB.	
570	Expected Results: the URDB is displayed.	
580	SMC CM Administrator: Updates the recommendation record to reflect ESDIS CCB's decision.	
590	Expected Results: URDB stores the information.	
Data Reduction and Analysis Steps:		
Signature:		**Date:**

8.4 Configuration Management Scenario

This scenario conducts the site operations staff through the ECS capability for performing system-level configuration management. Resource management procedures are evaluated for effective, complete and prompt coordination and movement between ECS sites, of resources, and resource related procedures and permissions, such as operational directives and COTS software usage licenses and unlicensed toolkits. The logistics management activities are assessed for their combined ability to monitor and communicate information concerning spares and consumable inventories and replenishment.

The completeness, effectiveness and the degree of comprehensives of the ECS capability for controlling and maintaining system-wide inventories including evaluation of previous or on-going inventory procedures is assessed. ECS system-level quality management is evaluated for its ability to assess overall ECS performance within the SMC, for effective SMC/LSM coordination, and for satisfactory LSM quality assurance procedures. The ECS capability for collecting controlling, maintaining and distributing ECS system-level policies and procedures is evaluated as well as the capability of providing, maintaining. and updating a bulletin board service for publishing current ECS status, events, news and toolkit references and updates. AT configuration management evaluations include assessment of the ECS network management capability for providing control of network configuration parameters and resources.

8.4.1 Resource Management Sequence

This sequence conducts the testers through ECS resource management activities for providing system-level information, equipment and software resources to the GSFC site. The site management and operations team demonstrates the SMC capability to generate and send ground operations events to sites for implementation, as well as the LSM capability for conveying, monitoring and reporting to the SMC on the status and progress of the implementation of these activities. The SMC procedures for making available system-level toolkits for automated distribution to the GSFC site is also inspected, including procedures for distributing unlicensed toolkit components, licenses for commercial products, product upgrades and user/maintenance documentation.

Configuration: The subsystem needed to perform this sequence of tests are as follows. CSS/MSS, DSS, INS, ISS, & PLS. Refer to Appendix D for additional detail.

External Interfaces: The external interfaces (i.e. other ECS sites and data sources) needed for this sequence (both real and simulated) are listed:

SMC

Operator Position(s): The operator positions from the ECS Maintenance and Operations Position Descriptions document (607-CD-001-002) needed to support this sequence are listed:

DAAC Operations Supervisor
DAAC Production Monitor
DAAC Computer Operator

Operational Scenario(s): The operations scenarios, taken from the Operations Scenarios for the ECS Project: Release-A document (605-CD-001-003), that were used to develop tests in this sequence of tests are listed:

Resource Planning Scenario (Section 3.7)
Resource Management and Control Scenario (Section 3.8)

Test Dependencies: The following table identifies the test procedure(s) in a sequence of tests that should be run prior to or concurrently with a sequence or test procedure.

Test Procedure No.	Site/Procedure No.	Comments
A080410.010$G	A080410.010$S	prior

8.4.1.1 Resource Management Directive

TEST Procedure No.: A080410.010$G	Date Executed:	Test Conductor:
Title:	Resource Management Directive	
Objective:	This test case investigates the SMC M&O staff's ability to generate managerial and operational directives, such as directives involving operational status, resource allocation and upgrade to the sites' LSM M&O procedures.	

Requirements	Acceptance Criteria
EOSD2660#A	This requirement is verified through demonstration. ECS elements shall at all times maintain and comply with the security directives issued by the SMC. The Tester demonstrates that the system provides the capability to view a security directive that was previously transmitted and stored in the database from the SMC.
SMC-2115#A	This requirement is verified through demonstration. The LSM shall convey for GSFC implementation, the managerial and operational directives regarding the allocation or upgrade of any hardware and scientific and systems software. The Tester demonstrates that the system provides the capability to display a policy, procedure, or directive that was previously transmitted and stored in the database from the SMC.

Test Inputs:

Data Set Name	Data Set ID	File Name	Description	Version
Resource Directives			Hard/soft copies	

Step-By-Step Procedures		
Step No.	**Input Action / Expected Results**	**Pass / Fail / Comments**
10	DAAC Computer Operator: Logon to the AIT workstation at the GSFC DAAC. The office automation tools must be available on the workstation.	
20	DAAC Computer Operator: Select the tools option from the menu.	
30	Expected Results: The tools menu is displayed.	
40	DAAC Computer Operator: Select the option for office automation.	
50	Expected Results: The office automation menu is displayed.	
60	DAAC Computer Operator: Select the option for GhostView and follow directions to view a document.	
70	note: To view a policy, procedure, or directive that was previously transmitted and stored in the database from the SMC. DAAC Computer Operator: Choose open under the file button and select the desired file to view.	
80	Expected Results: The selected file is displayed.	
90	DAAC Computer Operator: Select the print button.	
100	Expected Results: The selected file is printed.	
110	DAAC Computer Operator: Select close to close the desired file.	
120	DAAC Computer Operator: Select quit to exit the processor.	
130	Expected Results: The MSWindows Program Manager appears.	
140	note: To view the DAAC files for operational status, resource allocations, or any system upgrades. DAAC Computer Operator: Select the MSWindows option from under the Office Automation option.	
150	Expected Results: The MSWindows' Program Manager is displayed.	
160	DAAC Computer Operator: Select the file button.	
170	Expected Results: The file menu is displayed under a disk drive.	
180	DAAC Computer Operator: Select the correct disk drive and the file in either Microsoft Word or Excel format and select the open button to view the document.	
190	Expected Results: The document is displayed.	
200	DAAC Computer Operator: Select print to print the document if desired.	
210	DAAC Computer Operator: Insert or delete changes into the desired file, then select save.	
220	Expected Results: The changes are saved in the document.	

230	DAAC Computer Operator: To exit the processor select quit.	
240	Expected Results: The MSWindows program manager appears.	
250	DAAC Computer Operator: To end this test exit Windows.	
260	Expected Results: The SSIT Manger-Operator View is displayed.	
Data Reduction and Analysis Steps:		
Signature:		**Date:**

8.4.1.2 Sufficient Storage

TEST Procedure No.: A080410.040$L	**Date Executed:**	**Test Conductor:**
Title: Sufficient Storage		
Objective: This test confirms the capability of ECS to provide sufficient storage for the Client subsystem, Sustaining Engineering, and IV&V.		

Requirements	Acceptance Criteria
EOSD1140#A	This requirement is verified through analysis. ECS shall allocate 10% of development resources (the ECS Sustaining Engineering Facility at GSFC), including processing, storage, and networks, for the IV&V activity. Analytic and static analysis models along with daily performance reports are used to verify this requirement.
IMS-1790#A	This requirement is verified through analysis. The IMS shall provide, based upon the data model defined in Appendix C, sufficient storage for, at a minimum: a. Directory metadata b. Guide (documentation/reference material) metadata c. Inventory metadata d. System space, LSM data, and data base system overhead e. Metadata staging area f. Spacecraft housekeeping and ancillary data metadata g. Science processing library software metadata h. Summary data statistics i. User workspace This requirement is verified at the end of each day using log files and accounting report.

Test Inputs: There are no input data sets for this test procedure**.**

Step-By-Step Procedures		
Step No.	**Input Action / Expected Results**	**Pass / Fail / Comments**
	There are no step-by-step procedures.	
Data Reduction and Analysis Steps: A. Analytic and static analysis models along with daily performance reports from the Release A DAACs and EBnet will be used to verify the design of SMC to accommodate 100 percent growth in processing speed. B. Static analysis models along with daily performance reports from the Release A DAACs and EBnet will be used to verify the design of SMC to accommodate 100 percent growth in storage capacity. Performance reports from the Release A DAACs and EBnet are used for DAACs site and network trend analysis. The Tivoli and Openview tools are used at the SMC to determine resources impact.		
Signature:		**Date:**

8.4.2 Maintenance Management Sequence

This sequence is not applicable for the GSFC ECS DAAC Volume of the Acceptance Test Procedures document for Release A.

8.4.3 Logistics Management Sequence

This sequence reviews ECS capabilities for managing system-level logistics management activities and for managing system-level personnel and resources in logistics control activities. The AT team inspects SMC's procedures for developing and updating a system-level logistics management database containing historical, current and planned logistics commitments. The GSFC policies and procedures are inspected for the existence and completeness of procedures for receiving logistics management directives and for monitoring, status and reporting to SMC on GSFC activities in response to logistics related directives.

Configuration: The subsystem needed to perform this sequence of tests are as follows. CSS/MSS, DSS, INS, ISS, & PLS. Refer to Appendix D for additional detail.

External Interfaces: The external interfaces (i.e. other ECS sites and data sources) needed for this sequence (both real and simulated) are listed:

SMC

Operator Position(s): The operator positions from the ECS Maintenance and Operations Position Descriptions document (607-CD-001-002) needed to support this sequence are listed:

DAAC Operations Supervisor

DAAC Resource Manager

DAAC Computer Operator

Operational Scenario(s): There are no operations scenarios taken from the Operations Scenarios for the ECS Project: Release-A, used during this sequence of tests.

Test Dependencies: The following table identifies the test procedure(s) in a sequence of tests that should be run prior to or concurrently with a sequence or test procedure.

Test Procedure No.	Site/Procedure No.	Comments
none		

8.4.3.1 Logistics Monitoring

TEST Procedure No.: A080430.010$G	**Date Executed:**	**Test Conductor:**
Title: Logistic Monitoring		
Objective: This test case verifies that the LSM has the capability to monitor the spares and consumables inventory.		

Requirements	Acceptance Criteria
SMC-2305#A	This requirement is verified through demonstration. The LSM shall monitor the spares inventory within its element. The Tester demonstrates that the system provides the capability to use the LSM logistics monitoring procedure information, track the location, quantity, status, and consumption rate concerning spares and consumables.
SMC-2325#A	This requirement is verified through demonstration. The LSM shall monitor the consumable inventory within its element for items used by the system including, at a minimum: a. Computer tapes b. Computer disks c. Computer paper The Tester demonstrates that the system provides the capability to manually input the required list of consumables and a spare part to be displayed (computer tapes, disks, and paper), and record the quantity and status of three consumable items (computer tapes, computer disks, and computer paper) as contained in the data base.

Test Inputs: Lists of inventory for spares and consumables such as, computer tapes, disks, and paper.

Data Set Name	Data Set ID	File Name	Description	Version

Step-By-Step Procedures		
Step No.	**Input Action / Expected Results**	**Pass / Fail / Comments**
10	DAAC Computer Operator: Login to ECS	
20	DAAC Computer Operator: Open the Inventory file management directory.	
30	Expected Result: Inventory file is ready for access.	
40	DAAC Operations Supervisor: Using the LSM logistics monitoring procedure information, track the location, quantity, status, and consumption rate concerning spares and consumables.	
50	DAAC Operations Supervisor: Manually input the required list of consumables and spare part to be displayed (computer tapes, disks, and paper). Record the quantity and status of three consumable items (computer tapes, computer disks, and computer paper) as contained in the data base.	
60	Expected Result: All required characteristics for running the query is recorded and processed.	
70	DAAC Computer Operator: A physical inspection of the inventory is made at the site to obtain the actual quantity and status of the three consumable items.	
80	Expected Result: The inventory list of the computer consumables and spare part is the same as the result of the physical inspection.	
90	DAAC Computer Operator: Compare the computer generated inventory list with the test input supplied list.	
100	Expected Result: There is no discrepancies between the data base information and the quantity and status of consumable items and spare parts actually available at the site.	
110	DAAC Computer Operator: Record any missing inventory or discrepancy in the evaluation report. The lists should compare.	
120	Expected Result: The lists compare.	
Data Reduction and Analysis Steps:		
Signature:		**Date:**

8.4.3.2 Logistics Replenishment

TEST Procedure No.: A080430.020$G	Date Executed:	Test Conductor:
Title: Logistics Replenishment		
Objective: This test case verifies that the LSM has the capability to manage, replenishment of spare parts and consumable items.		

Requirements	Acceptance Criteria
SMC-2315#A	This requirement is verified through demonstration. The LSM shall manage the replenishment of spare parts within its element. The Tester demonstrates that the system provides the capability to replenish spare parts and consumable items.
SMC-2335#A	This requirement is verified through demonstration. The LSM shall manage the replenishment of consumable items for its element. The Tester demonstrates that the system provides the capability to replenish spare parts and consumable items.

Test Inputs: Lists of inventory for spares and consumables such as, computer tapes, disks, and paper.

Data Set Name	Data Set ID	File Name	Description	Version

Step-By-Step Procedures		
Step No.	**Input Action / Expected Results**	**Pass / Fail / Comments**
10	DAAC Operations Supervisor: Review the procedures for overseeing and managing, respectively, the replenishment of spare parts and consumable items.	
20	DAAC Computer Operator: Login to ECS.	
30	DAAC Computer Operator: Open the Inventory file management directory.	
40	Expected Result: Inventory file is ready for access.	
50	DAAC Computer Operator: Bring up the data base and change the current quantities of consumable items accordingly.	
60	DAAC Computer Operator: Manually input the required list of consumables and spare part to be displayed (computer tapes, disks, and paper).	
70	Expected Result: All required characteristics for running the query is recorded and processed.	
80	DAAC Computer Operator: List the consumables and spare part.	
90	Expected Result: The inventory list of the computer consumables and spare part is displayed.	
100	DAAC Computer Operator: Check consumable and spare part list for shortfalls.	
110	Expected Result: If a shortfall exists an alert or warning message will be generated and displayed. No shortfalls should exist.	
120	DAAC Computer Operator: Order any shortfall item.	
130	Expected Result: Change in the data base to indicate the items have been ordered.	
140	DAAC Computer Operator: Record any discrepancy in the new inventory list.	
Data Reduction and Analysis Steps:		
Signature:		**Date:**

8.4.4 Training Management Sequence

This sequence provides the methodology for the inspection of ECS capabilities for managing system-level training and for supplying system-level personnel and courseware in performing on-site courses. It inspects the established database architecture to confirm the SMC's ability for developing and updating a system-level training management information base containing historical, current and planned schedules courseware availability, training commitments and budgets pertaining to system training activities. The SMC training policy and procedures are inspected for specification of management activities for providing system-level assistance in managing site training.. The procedures, at GSFC, are inspected for the existence and completeness of procedures for receiving training management directives

and for monitoring, status and reporting to SMC on site activities in response to SMC originated training directives. The SMC training policies and procedures are inspected for specification of specific assistance activities in assisting and providing system-level skills and resources to assist in site-level training and courseware development, including personnel skills, multi-site training tools and system-level training courseware toolkits. The procedures, at GSFC, are inspected for the existence and completeness of procedures for applying available SMC training resources within their assigned facilities. SMC procedures for monitoring and evaluating training course conduct and training effectiveness at the system and site levels are inspected.

Configuration: The subsystem needed to perform this sequence of tests are as follows. CSS/MSS, DSS, INS, ISS, & PLS. Refer to Appendix D for additional detail.

External Interfaces: The external interfaces (i.e. other ECS sites and data sources) needed for this sequence (both real and simulated) are listed :

SMC

Operator Position(s): The operator positions from the ECS Maintenance and Operations Position Descriptions document (607-CD-001-002) needed to support this sequence are listed:

DAAC Operations Supervisor

DAAC Resource Manager

DAAC Computer Operator

Operational Scenario(s): There are no operations scenarios taken from the Operations Scenarios for the ECS Project: Release-A, used during this sequence of tests.

Test Dependencies: The following table identifies the test procedure(s) in a sequence of tests that should be run prior to or concurrently with a sequence or test procedure.

Test Procedure No.	Site/Procedure No.	Comments
A080640.030$G	A080640.030$S	concurrent

8.4.4.1 ECS Training and Certification Program Management

TEST Procedure No.: A080440.010$G	Date Executed:	Test Conductor:
Title:	ECS Training and Certification Program Management	
Objective:	The Training and Certification Program Management test verifies that the ECS SMC training facility develops plans for conducting training courses.	
Requirements	**Acceptance Criteria**	

SMC-2405#A	This requirement is verified through analysis. The LSM shall coordinate with the SMC in managing the training program for its element. The OA tools assists the SMC training staff in determining training requirements for various operator positions, tracking resources for training, and maintaining training course information. The OA tools support the management of training and certification programs for the ECS. Manually. Performed by M&O staff using phone, e-mail, or through access to site's training planning documents.
SMC-2415#A	This requirement is verified through analysis. The LSM shall receive from the SMC descriptions and schedules for training courses. Using the Training database, the SMC training staff uses the information to assist in the following planning activities: scheduling dates of training courses, developing training courses, scheduling training resources (system equipment, software, instructional materials), and scheduling personnel to support training. The ECS training database is updated with all of the scheduling information and formatted into a Training Schedule Report. This report is disseminated to the ECS site managers via the ECS training bulletin board as the proposed training schedule. Manually. Performed by M&O staff using e-mail and remote access to office automation tools.

Test Inputs: Written plans for conducting training and certification programs for the ECS.
Training database.

Data Set Name	Data Set ID	File Name	Description	Version

Step-By-Step Procedures		
Step No.	**Input Action / Expected Results**	**Pass / Fail / Comments**
10	DAAC Resource Manager: Review the procedures for the overseeing and managing of training and certification programs for ECS.	
20	Expected Result: The procedures determining training requirements for various operator positions, tracking resources for training, and maintaining training course information are reviewed.	
30	DAAC Computer Operator: Login to ECS.	
40	DAAC Computer Operator: Open the file from the SMC containing plans for conducting training and certification programs for ECS..	
50	Expected Result: File open and ready for access.	
60	DAAC Resource Manager: Using the site information on the personnel training needs, the number of people requiring training, and unique training requirements. Query the database for the purpose of scheduling a training course.	
70	Expected Result: Information is collected from the training database.	
80	DAAC Resource Manager: Schedule a training course from the SMC.	
90	Expected Result: The SMC training staff contacts the site DAAC Resource Manager, via Email, to obtain information on the personnel training needs, and the number of people requiring training.	
100	SMC Training Staff: Using the Training database, the information is accessed in the following planning activities: scheduling dates of training courses, developing training courses, scheduling training resources (system equipment, software, instructional materials), and scheduling personnel to support training.	
110	Expected Result: A training course is scheduled.	
120	SMC: The training database is updated with all of the scheduling information and formatted into a Training Schedule Report.	
130	Expected Result: The training schedule report is disseminated to the DAAC Resource Manager via the ECS training bulletin board as the proposed training schedule.	

140	Expected Result: Training registration for the course is done by Email. A confirmation of the training registration application is transferred via Email.	

Data Reduction and Analysis Steps:

After the information from GSFC has been entered into the Training database the following steps occur:

A. The SMC uses the information to assist in planning activities for scheduling dates of training courses, developing training courses, scheduling training resources (system equipment, software, and scheduling personnel to support training.

B. The training database is updated with scheduling information.

C. This information is disseminated to GSFC via the ECS training bulletin board as the proposed training schedule.

D. After review and consideration by GSFC, the SMC finalizes the training course schedule and makes it available via the ECS training bulletin board.

E. Training registration is done by Email. A confirmation of all training registration applications is transferred via Email.

Signature:	**Date:**

8.4.4.2 On-the-Job Training

This test procedure is not applicable for the GSFC Volume of the Acceptance Test Procedures document for Release A.

8.4.5 Inventory Management Sequence

This sequence provides the methodology for test inspection of ECS capabilities for providing and maintaining a configuration management (CM) system, maintaining inventory data bases, managing system-level inventory policy and procedures, and participating and contributing system-level skills and resources in performing site-level inventory activities. The tester inspects the SMC's procedures and policy for planning, establishing and maintaining a system-wide inventory of all hardware, science software, system software, and associated documentation within ECS.

Configuration : The subsystem needed to perform this sequence of tests are as follows. CSS/MSS, DSS, INS, ISS, & PLS. Refer to Appendix D for additional detail.

External Interfaces: The external interfaces (i.e. other ECS sites and data sources) needed for this sequence (both real and simulated) are listed :

SMC

Operator Position(s): The operator positions from the ECS Maintenance and Operations Position Descriptions document (607-CD-001-002) needed to support this sequence are listed:

DAAC Operations Supervisor

DAAC Resource Manager

DAAC Computer Operator

Operational Scenario(s): The operations scenarios, taken from the Operations Scenarios for the ECS Project: Release-A document (605-CD-001-003), that were used to develop tests in this sequence of tests are listed:

Configuration Management Scenario (Section 3.4)

Test Dependencies: The following table identifies the test procedure(s) in a sequence of tests that should be run prior to or concurrently with a sequence or test procedure.

Test Procedure No.	Site/Procedure No.	Comments
none		

8.4.5.1 Inventory and Configuration Management

TEST Procedure No.: A080450.010$G	**Date Executed:**	**Test Conductor:**
Title:	Inventory and Configuration Management	
Objective	To verify that the LSM can establish and maintain a system-wide inventory data base of hardware, system software, and science software and provide a system-wide configuration management (CM) capability.	

Requirements	Acceptance Criteria
DADS1850#A	This requirement is verified through demonstration. Each DADS shall utilize the configuration management toolkit provided by the SMC. The Tester shows that the system provides the capability for utilizing the configuration management toolkit provided by the SMC.
DADS1860#A	This requirement is verified through demonstration. Each DADS shall, in conjunction with the SMC, provide configuration management for its internal resources. The Tester shows that the system provides the capability for configuration management of its internal resources.
IMS-1380#A	This requirement is verified through test. The IMS shall provide the capability to integrate the element toolkits with a common user interface. The Tester tests that the system provides the capability to integrate the element toolkits with a common user interface.
SMC-2515#A	This requirement is verified through test. The LSM shall provide configuration management for at least the operational hardware, system software, and scientific software within its element and for the migration of enhancements into the operational system. The Tester tests that the system provides the capability for maintaining the inventory of hardware, science software, and system software on a system-wide basis.

Test Inputs: System inventory data base file of all the hardware, scientific and system software contained in the ECS.

Data Set Name	Data Set ID	File Name	Description	Version

Step-By-Step Procedures		
Step No.	**Input Action / Expected Results**	**Pass / Fail / Comments**
10	DAAC Operations Supervisor: Review the element and configuration management toolkits and the documentation for maintaining the inventory of hardware, science software, and system software on a system-wide basis.	
20	DAAC Computer Operator: Log onto a workstation.	
30	Expected Results: Successful login.	
40	DAAC Computer Operator: Bring up and access the data base, which contains CM information .	
50	DAAC Computer Operator: Check for the established SMC created inventory and configuration management files, using the Clearcase tool.	
60	Expected Result: The files will be identified and located for input/output.	
70	DAAC Computer Operator: Select data base information containing one hardware item .	
80	DAAC Computer Operator: Print the inventory log file information for the one hardware item that contains the, hardware ID numbers, version numbers and dates, manufacturer, part number, and serial number.	
90	Expected Result: The inventory file will be printed.	
100	DAAC Computer Operator: Inspect the identification numbers, manufacturer, part number, and serial number of the actual hardware item and record this information.	
120	Expected Result: The data base information compares with results of the hardware inspection. There should be no discrepancies between the information contained in the data base and the actual items selected for inspection.	
130	DAAC Computer Operator: Select data base information containing one software item .	
140	DAAC Computer Operator: Print the inventory log file information for the one software item that contains the, version numbers and dates, name and locator information for software maintenance, and the location where the software is used.	
150	Expected Result: The inventory file will be printed.	
160	DAAC Computer Operator: Inspect the version numbers and dates, name and locator information for software maintenance, and the location where the software is used.	
170	Expected Result: The data base information compares with results of the software inspection. There should be no discrepancies between the information contained in the data base and the actual item selected for inspection.	
Data Reduction and Analysis Steps:		
Signature:		**Date:**

8.4.5.2 LSM Enhancement Migration and Inventory Management

TEST Procedure No.: A080450.030$G	**Date Executed:**	**Test Conductor:**
Title:	LSM Enhancement Migration and Inventory Management	
Objective:	To verify the capability of the LSM to update the system-wide inventory data base and provide CM for the migration of upgrades and enhancements into the operational system for site-specific items.	

Requirements	**Acceptance Criteria**
SMC-2505#A	This requirement is verified through demonstration. The LSM shall update the system-wide inventory data base consisting of all hardware, system software, and scientific software contained within its element. The Tester demonstrates that the system provides the capability for updating the inventory data base for hardware and system and science software.

Test Inputs: Inventory data base file containing operational system upgrades and enhancements.

System must have a configuration management capability in place.

Data Set Name	**Data Set ID**	**File Name**	**Description**	**Version**

Step-By-Step Procedures		
Step No.	**Input Action / Expected Results**	**Pass / Fail / Comments**
10	DAAC Operations Supervisor: Review the documentation for updating the inventory data base for hardware and system and science software.	
20	DAAC Operations Supervisor: Use this information to update the data base containing CM information for hardware.	
30	DAAC Computer Operator: Log onto a workstation.	
40	Expected Results: Successful login.	
50	DAAC Operations Supervisor r: Check for the establishment of inventory and configuration management files, using the Clearcase tool load the inventory file.	
60	Expected Result: Inventory file will be loaded and ready for input/output.	
70	DAAC Computer Operator: Retrieve data base information about one specified hardware item .	
80	Expected Result: The identification number, manufacturer, part number, and serial number of the hardware item should be displayed.	
90	DAAC Operations Supervisor: Identify the hardware item to be replaced and provide the ID number, manufacturer, part number, and serial number of the new H/W item. Make the file change.	
100	Expected Result: The original H/W item will be replaced with the new one. This new H/W configuration will be reflected in the inventory data base with the identification number, manufacturer, part number, and serial number of the new hardware item.	
110	DAAC Operations Supervisor: Close out the inventory file.	
120	Expected Result: File will be closed.	
130	DAAC Computer Operator: Using Clearcase, load the CM file containing information about the system and science software data base.	
140	Expected Result: The S/W data base file is opened for I/O operations.	
150	DAAC Computer Operator: Print information for a selected processor from the system and science software data base file, which contains at a minimum the processor name, version, and maintenance performed.	
160	Expected Result: The selected processor information including processor name, version, and maintenance performed is printed.	
170	DAAC Operations Supervisor: Identify the software processor to be replaced and provide the processor name, version, and maintenance performed of the new S/W processor. Make the file change.	

180	Expected Result: The original software processor is replaced with the new one. This new S/W configuration will be reflected in the inventory data base with the processor name, version, and maintenance performed of the new software processor.	
190	DAAC Operations Supervisor: Inspect and compare the printed output with the current software configuration and record any discrepancies. There should not be any discrepancies.	
191	DAAC Operations Supervisor: Reset all data base items to there original values.	
200	Tester: Close the data base file.	
210	DAAC Computer Operator: Log off of the work station.	
Data Reduction and Analysis Steps:		
Signature:		**Date:**

8.4.5.3 SMC Enhancement Evaluation & Implementation Management

This test procedure is not applicable for the GSFC Volume of the Acceptance Test Procedures document for Release A.

8.4.6 Quality Management Sequence

This sequence illustrates to the tester ECS capabilities for establishing and maintaining quality assurance management data bases, for managing system-level quality assurance policy and procedures and for system-level quality assurance for overall ECS performance as well as for specific programmatic areas. The tester also inspects GSFC's procedures to confirm their ability to perform quality assurance for the site, such as site quality testing, benchmarks, audits of site enhancement implementations, site quality checking, processed and delivered quality checks and quality evaluations of site resource usage performance.

Configuration: The subsystem needed to perform this sequence of tests are as follows. CSS/MSS, DSS, INS, ISS, & PLS. Refer to Appendix D for additional detail.

External Interfaces: The external interfaces (i.e. other ECS sites and data sources) needed for this sequence (both real and simulated) are listed :

SMC

Operator Position(s): The operator positions from the ECS Maintenance and Operations Position Descriptions document (607-CD-001-002) needed to support this sequence are listed:

DAAC Operations Supervisor

DAAC Production Monitor

DAAC Computer Operator

DAAC Science Data Specialist

Operational Scenario(s): The operations scenarios, taken from the Operations Scenarios for the ECS Project: Release-A document (605-CD-001-003), that were used to develop tests in this sequence of tests are listed:

Performance Management Scenario (Section 3.5)

Test Dependencies: The following table identifies the test procedure(s) in a sequence of tests that should be run prior to or concurrently with a sequence or test procedure.

Test Procedure No.	Site/Procedure No.	Comments
none		

8.4.6.1 SMC Quality Assurance

This test procedure is not applicable for the GSFC Volume of the Acceptance Test Procedures document for Release A.

8.4.6.2 LSM Quality Assurance

TEST Procedure No.: A080460.020$G	**Date Executed:**	**Test Conductor:**
Title: LSM Quality Assurance		
Objective: To verify that the LSM has the capability to perform quality assurance (QA) activities.		

Requirements	Acceptance Criteria
SMC-3345#A	This requirement is verified through demonstration. The LSM must perform quality assurance for its site/elements performance as well as programmatic areas that includes, at a minimum: a. Quality testing, benchmarks and audits for element enhancement implementations. b. Quality checking and audits of products processed and delivered. c. Quality testing and audits of element resource performance. The Tester demonstrates that the system provides the capability for performing site-specific quality assurance, and that it has policies and procedures to ensure that quality testing, benchmarks and audits for site-specific enhancement implementations can be successfully accomplished, and that the quality testing and audits of DAAC resource performance can be performed.

Test Inputs: Data base file containing quality assurance information about system quality testing, benchmarks and audits.

The availability of performance management tools.

Data Set Name	Data Set ID	File Name	Description	Version
MET_001			Metadata	
QA_001			Quality Assurance	

Step-By-Step Procedures		
Step No.	**Input Action / Expected Results**	**Pass / Fail / Comments**
10	Data Specialist: Review the documentation for performing site-specific quality assurance and inspect policies and procedures to ensure that quality testing, benchmarks and audits for site-specific enhancement implementations can be successfully accomplished, and that the quality testing and audits of DAAC resource performance can be performed.	
20	Expected Result: Successful inspection.	
30	Data Specialist: Log onto a workstation.	
40	Expected Results: Successful login.	
	Note: Begin product quality assurance.	
50	Data Specialist: Request a data product (metadata file of simulated ingested data).	
60	Expected Result: The data server archives the product and sends a subscription notice.	
70	Data Specialist: Receives notification of the product and retrieves it from the data server for review.	
80	Expected Result: Product is reviewed and the quality is determined.	
90	Data Specialist: Updates the product metadata QA flag and requests the data server to archive the product.	
100	Expected Result: The data server archives the product and sends a subscription notice.	
110	Data Specialist: Receives notification of a new metadata QA flag attached to the product.	
	Note: Begin quality checking and auditing of products processed and delivered.	
120	Data Specialist: Requests a product retrieval through the data server.	
130	Expected Result: The product is made available from the data server.	
140	Production Monitor (QA); Performs manual QA on the product and sends a product archive request to the data server.	
150	Expected Result: The data server archives the product and sends out a subscription notice.	
160	Production Monitor (QA): Receives the notification.	
170	Expected Result: Accept notification and decide if any further action is needed.	
	Note: Begin performance management reporting	
180	Production Monitor (QA): Query the QA data base, select and print Performance Management report items about the above metadata product.	

190	Expected Result: Printed output containing product processing parameters, such as product size, archive space, media used, number of times distributed, CPU hours, line usage, etc.	
200	Production Monitor: Evaluate the product's quality using QA policies and procedures and perform actions necessary to reflect the appropriate quality assurance code in the product metadata.	
210	Production Monitor: Compare with the quality assurance documentation, recording any discrepancies and inadequacies.	
220	Production Monitor: Logoff the workstation	
Data Reduction and Analysis Steps:		
Signature:		**Date:**

8.4.7 Policies and Procedures Management Sequence

This sequence conducts an inspection of ECS/SMC/LSM procedures and policies for supporting, controlling and maintaining ECS/site policies and procedures covering site responsibility and authority, resource management, fault recovery, testing, simulation, maintenance, logistics, performance evaluation, training, quality and product issuance, inventory management, system enhancements, finance management, and administrative actions.

Configuration: The subsystem needed to perform this sequence of tests are as follows. CSS/MSS, DSS, INS, ISS, & PLS. Refer to Appendix D for additional detail.

External Interfaces: The external interfaces (i.e. other ECS sites and data sources) needed for this sequence (both real and simulated) are listed :

SMC

Operator Position(s): The operator positions from the ECS Maintenance and Operations Position Descriptions document (607-CD-001-002) needed to support this sequence are listed:

DAAC Operations Supervisor

DAAC Production Monitor

DAAC Computer Operator

Operational Scenario(s): The operations scenarios, taken from the Operations Scenarios for the ECS Project: Release-A document (605-CD-001-003), that were used to develop tests in this sequence of tests are listed:

Fault Management Scenario (Section 3.3)

Test Dependencies: The following table identifies the test procedure(s) in a sequence of tests that should be run prior to or concurrently with a sequence or test procedure.

Test Procedure No.	Site/Procedure No.	Comments
A080480.020$G	A080480.020$S	prior
A080480.010$G	A080480.010$S	prior

8.4.7.1 Policies and Procedures Control

TEST Procedure No.: A080480.010$G	**Date Executed:**	**Test Conductor:**
Title: Policies and Procedures Control		
Objective: To verify the overall support and control of policies and procedures affecting the ECS.		

Requirements	Acceptance Criteria
EOSD2100#A	This requirement is verified through inspection. Compliance for this requirement is demonstrated in DID 214/SE1. The ECS technical security policy planning shall be comprehensive and shall cover at least the following areas: a. Applicability of the C2 Level of Trustiness as defined by the NSA b. Applicability of the C2 Object Reuse capability c. Discretionary control and monitoring of user access d. ECS communications, network access, control, and monitoring e. Computer system "virus" monitoring, detection, and remedy f. Data protection controls g. Account/privilege management and user session tailoring h. Restart/recovery i. Security audit trail generation j. Security analysis and reporting k. Risk analysis The Operations Supervisor demonstrates by inspection that the security management policies and procedures at the site provides for password management, operational security, data classification, access privileges, system hardware and software maintenance, and spare parts inventory guidelines.
EOSD2200#A	This requirement is verified through inspection. Compliance for this requirement is demonstrated in DID 214/SE1. Selection criteria meeting overall ECS security policies and system requirements shall be applied when selecting hardware. The Operations Supervisor verifies through inspection that a security section is provided within all applicable documents at the site and is current with the ECS approved documentation.

Test Inputs: Copies of the policies and procedures affecting the ECS, such as, site authority, resource management, fault recovery, testing, simulations, maintenance, logistics, performance evaluation, training, quality and product assurance, inventory management, system enhancements, finance management, administrative actions, and security.

Step-By-Step Procedures		
Step No.	**Input Action / Expected Results**	**Pass / Fail / Comments**
10	Operations Supervisor: Confirm that the site receives system-level policies from the SMC. Verify that principal ECS operational functions at the site are provided for in the management and control of ESDIS/ECS policies and procedures.	
20	Operations Supervisor: Verify through inspection that the security management policies and procedures at the site includes password management, operational security, data classification, access privileges, system hardware and software maintenance, and spare parts inventory guidelines.	
30	Operations Supervisor: Confirms that the LSM uses methods and procedures appropriate for controlling policies and procedures as well as pertinent correspondence at the system-wide and site level, respectively.	
40	Operations Supervisor: Confirms that the policies and procedures are sufficiently expanded to provide a level of detail necessary for implementation at the site.	
50	Expected Results: Inspections and confirmations are successful. For specifics refer to DID611 and Zi014-00 Security Policy.	
60	Operations Supervisor: Verify through inspection that the ECS security policy covers the following areas, C2 level of security, communications, virus monitoring, protection controls, system restart/recovery, security audit trail generation, security analysis and reporting, and risk analysis.	
70	Expected Results: Inspection is successful. Specifics about compliance is demonstrated in DID 214/SE1.	
80	Operations Supervisor: Verify through inspection that the security section within all documents at the site are current with the ECS approved documentation.	
90	Expected Results: Inspection is successful.	
100	Operations Supervisor: Verify that backup copies of the policy and procedure manuals are maintained at a separate physical location at the site	
110	Expected Results: Verification is successful.	
Data Reduction and Analysis Steps:		
Signature:		**Date:**

8.4.7.2 Policies and Procedures Maintenance

TEST Procedure No.: A080480.020$G	**Date Executed:**	**Test Conductor:**
Title:	Policies and Procedures Maintenance	
Objective:	To verify that the LSM provides a bulletin board service with information on ECS status, events, and news so that ESDIS, SMC, and LSM policies and procedures and directives can be properly maintained and distributed. It confirms that access to updating this information is limited to specified personnel with the proper ECS responsibility and authority.	

Requirements	Acceptance Criteria
EOSD1990#A	This requirement is verified through inspection. The interpretation criteria for this requirement is as determined in the technical security planning policy activity documented in EOSD2100, and is verified in the previous procedure (A080480.010). The ECS system and elements shall employ security measures and techniques for all applicable security disciplines which are identified in the preceding documents. These documents must provide the basis for the ECS security policy. The Operations Supervisor verifies through inspection that there are security measures and techniques for all applicable security disciplines.
EOSD2100#A	This requirement is verified through inspection. The ECS technical security policy planning shall be comprehensive and shall cover at least the following areas: a. Applicability of the C2 Level of Trustiness as defined by the NSA b. Applicability of the C2 Object Reuse capability c. Discretionary control and monitoring of user access d. ECS communications, network access, control, and monitoring e. Computer system "virus" monitoring, detection, and remedy f. Data protection controls g. Account/privilege management and user session tailoring h. Restart/recovery i. Security audit trail generation j. Security analysis and reporting k. Risk analysis Verify through inspection that the security management policies and procedures at the site includes the ECS technical security policy planing.
EOSD2200#A	This requirement is verified through inspection. Selection criteria meeting overall ECS security policies and system requirements shall be applied when selecting hardware. The Tester will verify that the overall ECS security policies and system requirements are applied when selecting hardware.
SMC-2605#A	This requirement is verified through demonstration. Partial compliance is performed by the staff using various office automation, CM, and other tools. The LSM shall support the site and element in implementing ESDIS Project policies and procedures received from the SMC covering the following areas, at a minimum: a. Element responsibility and authority b. Resource management c. Fault recovery d. Testing

	e. Simulation f. Maintenance g. Logistics h. Performance evaluation i. Training j. Quality and product assurance k. Inventory management l. System enhancements m. Finance management n. Administrative actions o. Security The Operations Supervisor verifies through demonstration that the names for the policies, procedures, and directives for element responsibility and authority, resource management, fault recovery, testing, simulation, maintenance, logistics, training, inventory management, system enhancements, finance management, administrative actions, and security were received from the SMC.
SMC-2610#A	This requirement is verified through demonstration. Partial to support distribution of toolkits. The SMC shall provide and maintain a bulletin board service with information on ECS status, events, and news. The Operations Supervisor verifies through demonstration the capability of the LSM to provide, via the ECS bulletin board service, a toolkit consisting of a list of approved CASE tools and references to standards for exchanging data for science use.
SMC-4305#A	This requirement is verified through analysis. Compliance for this requirement is performed by using office automation tools. The LSM shall maintain fault management policies and procedures for its element. The Operations Supervisor verifies through analysis the capability of the system to find the policies, procedures, and directives for element responsibility and authority, resource management, fault recovery, testing, simulation, maintenance, logistics, training, inventory management, system enhancements, finance management, administrative actions, and security. Using the office automation tools, change a paragraph in the fault management directive and store the document back into the CM data base.
SMC-5305#A	This requirement is verified through analysis. In this release only partial compliance is performed using office automation tools. The LSM shall maintain security policies and procedures, including, at a minimum: a. Physical security b. Password management c. Operational security d. Data classifications e. Access/privileges f. Compromise mitigation The Operations Supervisor verifies through analysis the capability of the system to find the policies, procedures, and directives for physical security, password management, operational security, data classifications, access/privileges, and compromise mitigation. Using the office automation tools, change a paragraph in a security policy and store the document back into the CM data base.

Test Inputs:	Hardcopies of the ESDIS project policies and procedures which includes, element authority, resource management, fault recovery, testing, simulation, maintenance, logistics, performance evaluation, training, quality and product assurance, inventory management, system enhancements, finance management, administrative actions, and security.			
Data Set Name	**Data Set ID**	**File Name**	**Description**	**Version**

Step-By-Step Procedures		
Step No.	**Input Action / Expected Results**	**Pass / Fail / Comments**
10	Operations Supervisor: Login to the system.	
20	Expected Result: Successful logon.	
30	Operations Supervisor: Obtain proper ECS authority to update policies.	
40	Expected Result: The Tester has the responsibility and authority to access and update information in policies and procedures, and directives.	
50	Operations Supervisor: Enter the QA data base directory for read/write.	
60	Expected Result: Entry to the QA system.	
70	Operations Supervisor: Query the QA data base for on line policies and procedures, and directives.	
80	Expected Result: A listing of the current policies, procedures, and directives is displayed.	
90	Operations Supervisor: From the listing find the names for the policies, procedures, and directives for performance evaluation, and quality and product assurance.	
100	Operations Supervisor: Query the policy for performance evaluation and list the policy status.	
110	Operations Supervisor: Check known status with the computer generated policy status.	
120	Expected Result: The status information compares.	
130	Operations Supervisor: Using the office automation tools display the performance evaluation policy.	
140	Expected Result: The performance evaluation policy is displayed.	
150	Operations Supervisor: Using the office automation tools, change a paragraph in the policy and store the document back into the QA data base.	
160	Expected Result: The performance evaluation policy will be updated and flagged for down loading to the SMC to replace the document maintained in the SMC data base.	
170	Operations Supervisor: Close the QA data base.	
180	Operations Supervisor: Enter the CM data base directory for read/write.	
190	Expected Result: Entry to the CM system.	
200	Operations Supervisor: Query the CM data base for on line policies and procedures, and directives.	
210	Expected Result: A listing of the current policies, procedures, and directives is displayed.	

220	Operations Supervisor: From the listing find the names for the policies, procedures, and directives for element responsibility and authority, resource management, fault recovery, testing, simulation, maintenance, logistics, training, inventory management, system enhancements, finance management, administrative actions, and security	
230	Operations Supervisor: Query the policy for performance evaluation and list the directive status for training.	
240	Operations Supervisor: Check known status with the computer generated directive status.	
250	Expected Result: The status information compares.	
260	Operations Supervisor: Using the office automation tools display the training directive.	
270	Expected Result: The training directive is displayed.	
280	Operations Supervisor: Using the office automation tools, change a paragraph in the directive and store the document back into the CM data base.	
290	Expected Result: The training directive will be updated and flagged for down loading to the SMC to replace the document maintained in the SMC data base.	
300	Operations Supervisor: Close the CM data base.	
310	Operations Supervisor: Demonstrate the capability of the LSM to provide, via the ECS bulletin board service, a toolkit consisting of a list of approved CASE tools and references to standards for exchanging data for science use.	
320	Expected Result: Successful demonstration.	
330	Operations Supervisor: Log on to the bulletin board server.	
340	Expected Result: Bulletin board service is initialized.	
350	Operations Supervisor: Scroll down the bulletin board list for information on ECS status, events, and news.	
360	Operations Supervisor: Open the ECS status bulletin board.	
370	Expected Result: A list of the ECS status messages is displayed.	
380	Operations Supervisor: Select a message.	
390	Expected Result: The message is displayed.	
400	Operations Supervisor: Quit.	
410	Expected Result: Exit the bulletin board.	

Data Reduction and Analysis Steps:

To assure that complete security policies and procedures applicable to GSFC are in-place and are maintained within the SMC complex the following is done:

A. Written site policies and procedures are available.

B. Inspect the security documentation for applicability to GSFC. The inspection also verifies that GSFC security documentation is maintained to include latest security directives

Signature:	**Date:**

8.4.8 Network Management Sequence

This sequence confirms the ECS ability to support, control and maintain ECS network management information such as network configuration management, network fault management, network performance management, network security management at the GSFC DAAC. ECS network configuration management functions are inspected. Procedures for interoperability with the NSI to provide user access to the ECS are inspected.

Configuration: The subsystem needed to perform this sequence of tests are as follows. CSS/MSS, DSS, INS, ISS, & PLS. Refer to Appendix D for additional detail.

External Interfaces: There are no external interfaces needed for this sequence.

Operator Position(s): The operator position from the ECS Maintenance and Operations Position Descriptions document (607/OP2) needed to support this sequence is listed:

DAAC Resource Manager

Operational Scenario(s): The following scenarios, taken from Operations Scenarios for the ECS Project: Release-A (605/OP1), are used during this sequence of tests.

System Status Scenario (Section 3.14.3)

Test Dependencies: There are no test dependencies needed for this sequence of tests.

8.4.8.1 Network Configuration and Status

TEST Procedure No.: A080490.010$G	**Date Executed:**	**Test Conductor:**
Title:	Network Configuration and Status	
Objective:	The Network Status Test confirms the ability of the GSFC LSM staff to obtain configuration management information and the status of network resources, including data flow status information. Services provided by ECS include collecting information describing the state of the network subsystem and its communications resources. This test also verifies the ability to perform management functions which exercise control over the network configuration, parameters, and resources. These functions include access to and manipulation of network resources.	

Requirements	Acceptance Criteria
ASTER-1060#A	This requirement is verified through test. ECS shall provide support for Transport Control Protocol/Internet Protocol (TCP/IP) communications protocols to the U.S. Gateway for ASTER GDS communications. The Tester must perform TCP and IP communications tests provided by HP OpenView. **Add verification method to RTM in CCR.**
EOSD0780#A	This requirement is verified through demonstration. Each element shall be capable of being monitored during testing. The Tester must obtain system status using HP OpenView.
ESN-0620#A	This requirement is verified through test.

	The ESN shall include a network management function to monitor and control the ESN. The Tester must verify that HP OpenView provides the ability to monitor and control the network.
ESN-0640#A	This requirement is verified through test. The ESN shall include management functions at each ECS element, equipment or gateway within the ESN. The MSS Discovery Service must discover (via network protocol) new instances of managed objects, detect missing occurrences of managed objects, and report missing occurrences of managed objects.
ESN-0650#A	This requirement is verified through test. The ESN shall perform the following network management functions for each protocol stack implemented in any ECS element, and each communications facility: a. Network Configuration Management b. Network Fault Management c. Network Performance Management d. Network Security Management The Tester must utilize HP OpenView to obtain information on the system configuration and changes in the system configuration. This test does NOT verify parts b, c and d of the requirement.
ESN-0690#A	This requirement is verified through test. The ESN shall be capable of reconfiguration transparent to network users. **Needs further investigation. On ESDIS List.**
ESN-0750#A	This requirement is verified through test. The ESN shall provide statistical processing capabilities to allow extraction and tabulation of network performance data. The MSS performance management application service must log ECS performance data pertaining to ECS network components and operating system resources.
ESN-0780#A	This requirement is verified through test. The network elements including the Internet interfaces, shall have the capability to report, periodically and on an interactive basis, network statistics to the ESN network management function, including the following information: a. Network round trip delay b. Network reset and restart indications c. Outages and CRC errors d. Performance statistics The ISS physical components, and services must have the capability to be monitored via SNMP agents. This test does NOT verify part d of this requirement.
ESN-0790#A	This requirement is verified through test. The ESN shall include the following configuration management functions at a minimum: a. collect information describing the state of the network subsystem and its communications resources, b. exercise control over the configuration, parameters, and resources of the subsystem, and over the information collected, c. store the configuration information collected, and d. display the configuration information The MSS Maps/Collection Service must retain the status of managed objects and their relationship to symbols that comprise a graphical

	representation of the physical network topology. The MSS Fault Management Application Service must provide the capability to create, modify, delete and display graphical representations of a given network topology.
ESN-0800#A	This requirement is verified through test. The ESN shall be capable of displaying the local network configuration status related to each system locally, and for all systems at the ESN network management facility. The MSS must be capable of displaying the local network configuration status related to each system locally, and for all systems at the network management facility.
ESN-1030#A	This requirement is verified through demonstration. The ESN shall perform periodic testing of alternate communication capabilities to verify that they are operational. The Tester must demonstrate multiple tests of the communications system.
ESN-1060#A	This requirement is verified through test. The ESN performance management function shall provide the capability to evaluate the performance of ESN resources and interconnection activities. The MSS performance management application service must be capable of receiving operational state change notifications from network components, hosts, applications, and peripherals.
ESN-1070#A	This requirement is verified through test. The ESN shall provide the capability to perform the following functions, at a minimum: a. generate/collect network statistics b. control collection/generation of network statistics c. store system statistics and statistical histories d. display the system statistics e. track end-to-end transaction performance. The Tester must generate, control, display and store system and network statistics. This test does NOT verify part e of this requirement.
ESN-1140#A	This requirement is verified through test. The ESN shall provide protocol translation, termination, bridging and routing. The Tester performs IP, UDP, and SNMP protocol tests demonstration the ability to translate between multiple protocols. The Tester identifies bridges and routers using HP OpenView's configuration topology map.
ESN-1330#A	This requirement is verified through test. The ESN shall provide ISO/OSI data communications protocols and services specified in the GOSIP (see Figure 8-3) to external interfaces as required by the IRDs. The CSS must support the TCP and UDP communication protocols to communicate between the servers and the clients. The GOSIP services are not required in Release A.
ESN-1340#A	This requirement is verified through test. The ESN shall provide support for TCP/IP communications protocols and services to external interfaces as required by the IRDs. The MSS must support TCP/IP communications protocols and services to external interfaces as required by the IRDs. The GOSIP services are not required in Release A.
NSI-0020#A	This requirement is verified through test.

	NSI shall provide support for TCP/IP communication protocols and services to ESN. The NSI must support TCP/IP communications protocols and services to GSFC as required by the IRDs.

Step-By-Step Procedures		
Step No.	**Input Action / Expected Results**	**Pass / Fail / Comments**
10	Resource Manager: Log on to DAAC MSS Server as an administrator and execute the HP OpenView application.	
20	Expected Results: HP OpenView window is displayed on the screen. The HP OpenView window displays a map depicting the DAAC configuration.	
30	Resource Manager: Identify routers and gateways depicted in the map.	
35	Expected Results: The routers and gateways are displayed in the map.	
40	Resource Manager: Initialize an application being monitored by HP OpenView.	
50	Expected Result: The application is initialized.	
60	Resource Manager: Verify that the system recognizes the monitoring of the application.	
70	Expected Result: The system recognizes the monitoring of the application.	
80	Resource Manager: Exit from the application and verify that the system depicts the change.	
90	Expected Result: The change is depicted by the system.	
100	Resource Manager: Make HP OpenView's window active by clicking on it.	
110	Expected Result: HP OpenView's window is active.	
120	Resource Manager: Perform an IP protocol test.	
130	Expected Result: HP OpenView verifies the use of IP protocol communications.	
140	Resource Manager: Perform a TCP protocol test.	
160	Expected Result: HP OpenView verifies the use of TCP protocol communications.	
170	Resource Manager: Perform an UDP protocol test.	
180	Expected Result: HP OpenView verifies the use of UDP protocol communications.	
190	Resource Manager: Perform an SNMP protocol test.	
200	Expected Result: HP OpenView verifies the use SNMP protocol communications.	
210	Resource Manager: Connect a hardware device to the network (e.g. a printer). Verify that the system recognizes the new configuration.	
220	Expected Result: The topology map displayed by HP OpenView depicts the new configuration.	
230	Resource Manager: Turn off the power to the hardware device. Verify that the system recognized the new configuration.	
240	Expected Result: The topology map displayed by HP OpenView depicts the new configuration.	

250	Resource Manager: Turn the power back on for the hardware device. Verify that the system recognized the new configuration.	
260	Expected Result: The topology map displayed by HP OpenView depicts the new configuration.	
270	Resource Manager: Disconnect the hardware device from the network. Verify that the system recognizes the new configuration.	
280	Expected Result: The topology map displayed by HP OpenView depicts the new configuration.	
290	Resource Manager: Change to the directory which contains the history log.	
300	Resource Manager: Examine the history log to determine whether the events have been documented.	
310	Expected Results: The events have been documented in the history log.	
Data Reduction and Analysis Steps:		
Signature:		**Date:**

8.4.8.2 Directory Service

TEST Procedure No.:	Date Executed:	Test Conductor:
A080490.050$G		

Title: Directory Service

Objective: The purpose of this test is to verify the functionality of the Directory/Naming Service. The Directory/Naming Service uniquely associates a name with resources/principals, either physical or logical, along with some information so they can be identified and located by the name even if the named resource changes its physical address over time.

Requirements	Acceptance Criteria
ESN-0010#A	This requirement is verified through test. ESN shall provide the following standard services: a. Data Transfer and Management Services b. Electronic Messaging Service c. Remote Terminal Service d. Process to Process Communication Service e. Directory and User Access Control Service f. Network Management Service g. Network Security and Access Control Service h. Internetwork Interface Services i. Bulletin Board Service The Tester verifies the directory and user access control service by defining an attribute using the Directory/Naming Service. This test does NOT verify parts a, b, c, d, f, g, h, and i of the requirement.
ESN-0490#A	This requirement is verified through test. The ESN shall provide a name-to-attribute mapping Directory Service. The Tester verifies the name-to-attribute mapping by defining an attribute using the Directory/Naming Service.
ESN-0510#A	This requirement is verified through test. The directory function shall be able to respond to requests for information concerning named objects, either physical or logical, so as to support communications with those objects. The Tester verifies the directory function by modifying an attribute definition using the Directory/Naming Service.
ESN-0590#A	This requirement is verified through test. The ESN Directory Service shall be protected by access control capabilities. The CSS Security service must provide an API to verify the identity of users.
ESN-0600#A	This requirement is verified through test. The ESN Directory service shall include services and supporting mechanisms to authenticate the credentials of a user for the purpose of granting access rights and authorizing requested operations. The CSS Security service must provide an API to check the authorization privileges of principals to access/control services/resources.
ESN-0610#A	This requirement is verified through test. The ESN shall include multiple Directory Service Agents (DSAs) which are collectively responsible for holding or retrieving all

	directory information which is needed by ECS. The Tester verifies the directory and user access control service by defining an attribute using the Directory/Naming Service.

Test Inputs:

Data Set Name	Data Set ID	File Name	Description	Version
ATTR_001			List of defined attributes	

Step-By-Step Procedures		
Step No.	**Input Action / Expected Results**	**Pass / Fail / Comments**
10	Resource Manager: Login to Client	
20	Expected Results: Client Desktop displays on the screen.	
30	Resource Manager: Perform DCE login using a DCE account and password.	
40	Expected Result: The Computer Operator gains access to the DCE account.	
50	Resource Manager: Type **cdsbrowser &** to verify the directory naming activity.	
60	Expected Result: The directory naming activity is verified.	
70	Resource Manager: From the cdsbrowser, select an attribute and press **Display**.	
80	Expected Result: The system is displays the attributes currently entered into the system.	
90	Resource Manager: Select **Attribute** and press **Display**.	
100	Expected Results: A list of available attributes is displayed on the screen.	
110	Resource Manager: Select the attribute **MSSAttr** to read the attribute values.	
120	Expected Results: The **MSSAttr** attribute values are displayed on the screen.	
130	Resource Manager: Verify a list of attribute types.	
140	Expected Results: Each of the attributes is contained in the list.	
150	Resource Manager: Select **Modify an Attribute**.	
160	Expected Results: Access to modify an attribute is available.	
170	Resource Manager: Change the **MSSAttr** attribute to **CSSAttr**.	
180	Expected Results: The name of the **MSSAttr** attribute is changed to **CSSAttr**.	
Data Reduction and Analysis Steps:		
Signature:		**Date:**

8.5 Performance Management Scenario

This scenario walks GSFC operations personnel through the process of accessing and displaying system performance parameters and metrics. It carries the staff through a series of analytical and diagnostic sequences which demonstrate the system's capability to measure GSFC performance and detect operational trends.

The Performance Management Scenario's acceptance testing activity confirms those functions that provide global integrated ECS performance management services and exercise system-wide

control. Verifying ECS metrics confirms ECS capability for defining meaningful measures, for developing and maintaining standard performance metrics, and for accomplishing system-level performance testing and performance improvement actions.

8.5.1 Metrics Sequence

This test sequence verifies the capability of the GSFC LSM to interact with the SMC to evaluate system performance. LSM capabilities, including the ability to implement SMC performance criteria and limits testing, using SMC data base metrics for comparison, are confirmed. The SMC and the LSM capabilities to generate alert indicators for fault and degraded conditions are also confirmed.

Finally, the capability of the GSFC DAAC to provide the required availability of key services and to switch over or repair failed capabilities within specified mean down times (MDTs) is confirmed.

Configuration: The subsystem needed to perform this sequence of tests are as follows. CSS/MSS, DSS, INS, ISS, & PLS. Refer to Appendix D for additional detail.

External Interfaces: The external interfaces (i.e. other ECS sites and data sources) needed for this sequence (both real and simulated) are listed:

SMC

Operator Position(s): The operator positions from the ECS Maintenance and Operations Position Descriptions document (607/OP2) needed to support this sequence are listed:

SMC Performance Analyst

DAAC Production Monitor

DAAC Resource Manager

Operational Scenario(s): The operations scenarios, taken from the Operations Scenarios for the ECS Project: Release-A document (605/OP1), that were used to develop tests in this sequence of tests are listed:

User Notes Performance Degradation (Section 3.5.2) - A080510.010$G

Operation Support Scenario (Section 3.5.1) - A080510.020$G

Test Dependencies: The following table identifies the test procedure(s) for this sequence of test that should be run prior to or concurrently with this test procedure.

Test Procedure No.	Site/Procedure No.	Comments
A080510.010$G	A080510.010$S	Concurrent
A080510.030$G	A080510.020$G	Concurrent

8.5.1.1 Performance Metrics Establishment

TEST Procedure No.:	Date Executed:	Test Conductor:
A080510.010$G		

Title: Performance Metrics Establishment

Objective: This test case verifies the capability of the SMC and the local site LSMs to establish, maintain and update system performance criteria and performance parameter limits and thresholds. The capability to establish multiple threshold levels, including on/off, pass/fail, and various levels of degradation, is also confirmed.

Requirements	Acceptance Criteria
ESN-1090#A	This requirement is verified through test. The ESN shall provide the capability to control the communications performance parameters of the network. On ESDIS List.
SMC-3355#A	This requirement is verified through analysis. The LSM shall implement the performance criteria from SMC (including parametric limits and operational threshold levels) for evaluating element resource performance During this test, LSM capabilities to set thresholds sent by the SMC will be verified by bringing up the appropriate tools and setting selected thresholds.
SMC-3375#A	This requirement is verified through test. For each limit checked parameter, the LSM (including those thresholds directed by the SMC) shall have the capability of evaluating multiple levels of thresholds including, at a minimum: a. On/off b. Pass/fail c. Various levels of degradation During this test, LSM capabilities to set thresholds sent by the SMC will be verified by bringing up the appropriate tools and setting each of the thresholds.
SMC-3385#A	This requirement is verified through test. **(RTM:analysis)** The LSM shall evaluate system performance against the ESDIS project established performance criteria. During this test, LSM capabilities to monitor system performance against ESDIS project performance criteria sent via the SMC will be verified by bringing up performance monitoring tools and demonstrating that these tools are capable of monitoring the specified performance parameters.

Test Inputs: Required test case inputs include a list of ESDIS-specified performance parameters, specifications, and policies and procedures, as well as an operational script exercising different levels of performance to assess the capability to update and check limit and threshold parameters.

Data Set Name	Data Set ID	File Name	Description	Version

Step-By-Step Procedures		
Step No.	**Input Action / Expected Results**	**Pass / Fail / Comments**
10	DAAC Production Monitor: Starts HP OpenView.	
20	Expected Result: OpenView window displays top level system map.	
30	DAAC Production Monitor: Selects an MSS managed host and set two thresholds for CPU utilization, one to indicate degraded performance and the other to indicate failure.	
40	Expected Result: The new CPU utilization threshold values can be observed by examining the Management Information Base (MIB).	
50	DAAC Production Monitor: Starts a script to cause the CPU utilization to exceed the threshold for degraded performance but not to exceed the upper (failure) limit.	
60	Expected Result: The MSS managed host is running in a degraded state due to heavy CPU utilization.	
70	DAAC Production Monitor: Clicks on CPU LOAD option from HP OpenView for MSS managed host.	
80	Expected Result: HP OpenView displays a CPU LOAD Graph containing the average CPU load on that host.	
90	DAAC Production Monitor: Clicks on TIME INTERVAL option from HP OpenView menu for that host and scrolls back to the time period when the lower CPU utilization threshold is exceeded (but not the upper limit).	
100	Expected Result: HP OpenView displays a CPU LOAD Graph containing the raised CPU load level .	
110	DAAC Production Monitor: Starts a script to cause the upper limit threshold to be exceeded.	
120	Expected Result: System is running MSS managed host exceeding its upper (failure) limit CPU utilization threshold thus causing a failure on the MSS managed host.	
130	DAAC Production Monitor: Clicks on CPU LOAD option from HP OpenView for MSS managed host.	
140	Expected Result: HP OpenView displays a CPU LOAD Graph containing the average CPU load on that host.	
150	DAAC Production Monitor: Clicks on TIME INTERVAL option from HP OpenView menu for that host and scrolls back to the time period that the upper limit CPU utilization threshold is exceeded.	
160	Expected Result: HP OpenView displays a CPU LOAD Graph containing the upper level of CPU load exceeded the currently configured CPU threshold thus causing the MSS managed host to fail. The HP OpenView icon for the MSS managed host is in red.	
170	DAAC Production Monitor: Repeats steps 10 - 160 using the Memory utilization performance parameter.	

180	Expected Result: As indicated in steps 10 - 160 but memory utilization now exceeds thresholds for degraded performance and later for failure).	
	THRESHOLDS DIRECTED BY THE SMC	
190	SMC Performance Analyst: Repeats steps 10 - 160 using SMC to set thresholds.	
200	Expected Result: As indicated in steps 10 - 160 but Performance Analyst at SMC now sets the thresholds for GSFC site performance.	

Data Reduction and Analysis Steps:

Expected results include the verification of the capability of the SMC and the site LSMs to establish, maintain and update system performance parameters and limit thresholds. The capability to monitor performance and to evaluate performance and any degradation with respect to these parameters will be confirmed.

Signature:	**Date:**

8.5.1.2 Performance Measurement and Degradation Response Capability

TEST Procedure No.:	**Date Executed:**	**Test Conductor:**
A080510.020$G		

Title:	Performance Measurement and Degradation Response Capability
Objective:	This test case verifies the capability of the GSFC DAAC site LSM to generate alert indicators for fault or degraded conditions and to generate corrective actions in response to these faults or degradations.

Requirements	**Acceptance Criteria**
SMC-3395#A	This requirement is verified through test. The LSM shall generate, in response to each limit check threshold, alert indicators of fault or degraded conditions. During the test, conditions will be created to trigger alert indicators for each limit checked threshold. The requirement will be verified after the selected limit checked thresholds have been exceeded and appropriate alerts generated.

Test Inputs:	Required test case inputs include performance parameters and specifications, and an operational script for exercising and simulating faults and degraded performance conditions. ESDIS policies and procedures specifying the range of responses and corrective actions to faults and performance degradation are also needed.

Data Set Name	**Data Set ID**	**File Name**	**Description**	**Version**

Step-By-Step Procedures		
Step No.	**Input Action / Expected Results**	**Pass / Fail / Comments**
10	DAAC Production Monitor: Starts the Management Information Base (MIB) initialization program using the input configuration file.	
20	Expected Result: The performance thresholds and system responses specified in the input configuration file are generated.	
30	DAAC Production Monitor: Clicks on HP OpenView Browse MIB option.	
40	Expected Result: HP OpenView shows the performance thresholds and system responses specified in the input configuration file.	
50	DAAC Production Monitor: Starts a production run of a PGE process on DMGHW-GSFC-2 that uses excessive disk space and causes the free space on DMGHW-GSFC-2 to fall below the threshold.	
60	Expected Result: A warning message indicating that free disk space on DMGHW-GSFC-2 has fallen below the threshold is displayed on the SMC operator's screen.	
70	DAAC Production Monitor: Double clicks on the GSFC icon on HP OpenView .	
80	Expected Result: HP OpenView displays GSFC submap.	
90	DAAC Production Monitor: Clicks on DMGHW-GSFC-2 icon.	
100	Expected Result: HP OpenView highlights the icon.	
110	DAAC Production Monitor: Selects the Browse MIB option to determine the problem.	
120	Expected Result: HP OpenView shows information on various MIB parameters, including degraded state of disk free space.	
130	DAAC Production Monitor: Graphs available disk free space data.	
140	Expected Result: HP OpenView graph capability shows that there has been excessive disk utilization since the process of Step 10 was started.	
150	DAAC Production Monitor: Terminate the process started in Step 50.	
160	Expected Result: The PGE process is terminated.	
170	DAAC Production Monitor: Saves the associated disk file to temporary storage.	
180	Expected Result: The disk file is backed up.	
190	DAAC Production Monitor: Deletes the associated disk file.	
200	Expected Result: The disk file is deleted.	
210	DAAC Production Monitor: Clicks on HP OpenView Browse MIB option.	

220	Expected Result: HP OpenView shows that DMGHW-GSFC-2 disk free space is no longer in a degraded state.	
230	DAAC Production Monitor: Clicks on the HP OpenView Update MIB option.	
240	Expected Result: HP OpenView displays current values for MIB parameters.	
250	DAAC Production Monitor: Updates performance criteria for response time, updates deficiency response to change color of the icon for the node responsible for the activity.	
260	Expected Result: Inspection of the MIB shows that the information has been updated.	
270	DAAC Production Monitor: Restarts a production run of a PGE process on DMGHW-GSFC-2 (step 50) without using excessive disk space.	
280	Expected Result: When the specified response time is exceeded, the specified icon will change color.	
290	DAAC Production Monitor: Repeats steps 240-280, goes through each of the remaining parameters indicated on the MIB.	
300	Expected Result: As indicated in steps 240-280.	
Data Reduction and Analysis Steps: Expected results include the verification of the capability of the site LSMs to monitor performance and to generate corrective actions for performance degradation and system faults.		
Signature:		**Date:**

ECS Segment	ECS Function or Service Provided	Minimum Availability/Maximum MDT
Overall	System-level Functions and Services	0.96/ 4 hr's.
SDPS	Receiving Science Data	0.999/ 2 hr's.
SDPS	Archiving and Distributing Data	0.98/ 2 hr's.
SDPS	User Interfaces to Information Management System (IMS) Services at DAAC Sites	0.993/ 2 hr's.
SDPS	Information Searches on the ECS Directory	0.993/ 2 hr's.
SDPS	Metadata Ingest and Update	0.96/ 4 hr's.
SDPS	Information Searches on Local Holdings	0.96/ 4 hr's.
SDPS	Local Data Order Submission	0.96/ 4 hr's.
SDPS	Data Order Submission Across DAACs	0.96/ 4 hr's.
SDPS	IMS Data Base Management and Maintenance Interface	0.96/ 4 hr's.
SDPS	Product Generation Capability (Each Computer)	0.95/ N/A
CSMS	SMC Capability to Gather and Disseminate System Management Information (for critical services)	0.998/ 20 min.

8.5.1.3 RMA Assurance Test and Analysis

TEST Procedure No.: A080510.030$G	**Date Executed:**	**Test Conductor:**
Title:	RMA Assurance Test and Analysis	
Objective:	This test case verifies the capability of the ECS to provide services with required reliability, maintainability and availability (RMA). It confirms the capability of the ECS to correct faults and to restore system capabilities within specified times. GSFC 420-05-03, Performance Assurance Requirements for the EOSDIS is the primary RMA Program Plan and , MIL-HDBK-217F, Reliability Prediction of Electronic Equipment, and MIL-HDBK-472, Maintainability Prediction, Procedure IV, provide guidelines in verifying ECS RMA. Table 8-1 summarizes key availability and maximum Mean Down Time (MDT) requirements for specific ECS services verified by this test case.	

Requirements	Acceptance Criteria
EOSD3490#A	This requirement is verified through inspection. (**RTM: demo)** Reliability statistics for ECS shall be collected and monitored using the Mean Time Between Maintenance (MTBM) for each component and operational capability. This capability is demonstrated by inspection of the MTBM Predictions used in, and analysis results documented in the DID #515. The inspection of process and procedures to collect and analyze RMA data during system operations after RRR will verify that Mean Time Between Maintenance MTBM will be collected and monitored.
EOSD3492#A	This requirement is verified through inspection. RMA data shall be maintained in a repository accessible for logistics analysis and other purposes.

	This capability is demonstrated by inspection of the RMA database documented in the approved DIDs #516 and #518.
EOSD3500#A	This requirement is verified through inspection. The ECS RMA Program shall adhere to GSFC 420-05-03, Performance Assurance Requirements for the EOSDIS. This capability is demonstrated by inspection of RMA Program Plan which is Section 7.0 of the approved Performance Assurance Implementation Plan DID #501.
EOSD3510#A	This requirement is verified through inspection. Reliability predictions shall be calculated in accordance with the parts count analysis method, Appendix A, of MIL-HDBK-217F, Reliability Prediction of Electronic Equipment. This capability is demonstrated by inspection of the prediction process and Reliability prediction values in the approved DID #516.
EOSD3600#A	This requirement is verified through inspection. Maintainability shall be predicted in accordance with MIL-HDBK-472, Maintainability Prediction, Procedure IV. This capability is demonstrated by inspection of the prediction process and Maintainability prediction values in the approved DID #518.
EOSD3620#A	This requirement is verified through inspection. (**RTM: analysis)** ECS shall predict and periodically assess maintainability by measuring the actual MDT and comparing to the required MDT. The prediction requirement is demonstrated by inspection of the process and prediction values in the approved DID #515 and #518. The assessment requirement of the actual MDT is demonstrated by inspection of the process and procedures to collect and analyze RMA data during system operations after RRR .
EOSD3625#A	This requirement is verified through inspection. For ECS functions with a backup capability, ECS shall use switchover time to the backup capability in measuring maintainability, rather than down time, when the component goes down. This requirement is demonstrated by inspection of the approved DID #515.
EOSD3630#A	This requirement is verified through inspection. (**RTM: analysis)** The maximum down time shall not exceed twice the required MDT in 99 percent of failure occurrences. This requirement will be demonstrated by inspection of the actual MDT data when the system has been in operation for a statistically significant length of time. (Note: This requirement is not verifiviable until the system has been in operation for a statistically significant length of time.) This requirement is not verifiable until the system has been in operation for a statistically significant length of time.
EOSD3700#A	This requirement is verified through inspection. (**RTM: analysis**) ECS functions shall have an operational availability of 0.96 at a minimum (.998 design goal) and an MDT of four (4) hours or less (1.5 hour design goal), unless otherwise specified. The above requirement covers equipment including: a. "Non-critical" equipment configured with the critical equipment supporting the functional capabilities in the requirements. b. Equipment providing other functionality not explicitly stated in the RMA requirements that follow.

	This requirement is demonstrated by inspection of the approved DID #515.
EOSD3900#A	This requirement is verified through inspection. (**RTM: analysis)** The SDPS function of receiving science data shall have an operational availability of 0.999 at a minimum (.99995 design goal) and an MDT of two (2) hours or less (8 minutes design goal). This requirement is demonstrated by inspection of the approved DID #515.
EOSD3910#A	This requirement is verified through test. The switchover time from the primary science data receipt capability to a backup capability shall be 15 minutes or less (10 minutes design goal). This requirement is demonstrated by the Maintainability Demonstration Test defined in DIDs #511 and #512 and documented in the Report DID 519.
EOSD3920#A	This requirement is verified through inspection. (**RTM: analysis)** The SDPS function of archiving and distributing data shall have an operational availability of 0.98 at a minimum (.999999 design goal) and an MDT of two (2) hours or less (9 minutes design goal). This requirement is demonstrated by inspection of the approved DID #515.
EOSD3930#A	This requirement is verified through inspection. (**RTM: analysis**) The user interfaces to Information Management System (IMS) services at individual Distributed Active Archive Center (DAAC) sites shall have an operational availability of 0.993 at a minimum (.9997 design goal) and an MDT of two (2) hours or less (1.6 hour design goal). This requirement is demonstrated by inspection of the approved DID #515.
EOSD3940#A	This requirement is verified through inspection. (**RTM: blank**) The SDPS function of Information Searches on the ECS Directory shall have an operational availability of 0.993 at a minimum (.9997 design goal) and an MDT of two (2) hours or less (1.4 hour design goal). This requirement is demonstrated by inspection of the approved DID #515.
EOSD3960#A	This requirement is verified through inspection. (**RTM: analysis)** The SDPS function of Metadata Ingest and Update shall have an operational availability of 0.96 at a minimum (.999999 design goal) and an MDT of four (4) hours or less (6 minutes design goal). This requirement is demonstrated by inspection of the approved DID #515.
EOSD3970#A	This requirement is verified through inspection. (**RTM: analysis)** The SDPS function of Information Searches on Local Holdings shall have an operational availability of 0.96 at a minimum (.999999 design goal) and an MDT of four (4) hours or less (6 minutes design goal). This requirement is demonstrated by inspection of the approved DID #515.
EOSD3980#A	This requirement is verified through inspection. **RTM:analysis** The SDPS function of Local Data Order Submission shall have an operational availability of 0.96 at a minimum (.999999 design goal) and an MDT of four (4) hours or less (6 minutes design goal). This requirement is demonstrated by inspection of the approved DID #515.

EOSD3990#A	This requirement is verified through inspection. **(RTM: analysis)** The SDPS function of Data Order Submission Across DAACs shall have an operational availability of 0.96 at a minimum (.999999 design goal) and an MDT of four (4) hours or less (6 minutes design goal). This requirement is demonstrated by inspection of the approved DID #515.
EOSD4000#A	This requirement is verified through inspection. (**RTM: analysis**) The SDPS function of IMS Data Base Management and Maintenance Interface shall have an operational availability of 0.96 at a minimum (.999999 design goal) and an MDT of four (4) hours or less (6 minutes design goal). This requirement is demonstrated by inspection of the approved DID #515.
EOSD4010#A	This requirement is verified through inspection. **(RTM: analysis)** Each computer providing product generation shall have an operational availability of 0.95 at a minimum (.9995 design goal). This requirement is demonstrated by inspection of the approved DID #515.
EOSD4100#A	This requirement is verified through test. **(RTM: Demo)** The ECS segments, elements, and components shall include the on-line (operational mode) and off-line (test mode) fault detection and isolation capabilities required to achieve the specified operational availability requirements. This requirement is demonstrated by the Maintainability Demonstration Test defined in DIDs #511 and #512 and documented in the Report DID 519..

Test Inputs: Test case inputs include reliability data and repair specifications for key ECS components, switch over time estimations, in-the-field maintenance records, and demonstrations by operations staff of repair and switch over procedures for various failure occurrences.

Data Set Name	Data Set ID	File Name	Description	Version

Step-By-Step Procedures		
Step No.	**Input Action / Expected Results**	**Pass / Fail / Comments**
10	DAAC Resource Manager: Inspects DID #515 to verify the following requirements: EOSD3490#A, EOSD3620#A, EOSD3625#A, EOSD3700#A, EOSD3900#A, EOSD3920#A, EOSD3930#A, EOSD3940#A, EOSD3960#A, EOSD3970#A, EOSD3980#A, EOSD3990#A, EOSD4000#A, EOSD4010#A.	
20	Expected Result: The expected result for each requirement is as stated in the acceptance criteria for each respective requirement.	
30	DAAC Resource Manager: Inspects DID #516 for the following requirements: EOSD3492#A, EOSD3510#A.	
40	Expected Result: The expected result for each requirement is as stated in the acceptance criteria for each respective requirement.	
50	DAAC Resource Manager: Inspects DID #518 for the following requirements: EOSD3492#A, EOSD3600#A, EOSD3620#A.	
60	Expected Result: The expected result for each requirement is as stated in the acceptance criteria for each respective requirement.	
70	DAAC Resource Manager: Inspects DID #501 for the following requirements: EOSD3500#A.	
80	Expected Result: The expected result for each requirement is as stated in the acceptance criteria for each respective requirement.	
90	DAAC Resource Manager: Examines the test executed in Maintainability Demo Test, DID #511 and DID #512 to verify that the switchover time from the primary science data receipt capability to a backup capability will take 15 minutes or less (EOSD3910#A).	
100	Expected Result: DID #519 (Test Report) states that the result of the test stated in DID #511 and DID #512 indicating that the switchover from the primary science data receipt capability to a backup capability takes 15 minutes or less.	
110	DAAC Resource Manager: Examines the test executed in Maintainability Demo Test, DID #511 and DID #512 to verify that the ECS system includes the on-line (operational mode) and off-line (test mode) fault detection and isolation capabilities required to achieve the specified operational availability (EOSD4100#A).	

120	Expected Result: DID #519 (Test Report) states that the result of the test stated in DID #511 and DID #512 indicating the ECS system includes the on-line (operational mode) and off-line (test mode) fault detection and isolation capabilities required to achieve the specified operational availability.	
Data Reduction and Analysis Steps: Expected results include inspecting the related Maintainability Demo Test documents to confirm that the ECS can make needed services available as required and can repair or switch over from failed capabilities.		
Signature:		**Date:**

8.5.2 Performance Monitoring, Analysis & Testing Sequence

This sequence guides the reviewer in confirming each LSM's (including the GSFC's) capabilities to generate, as needed, requests for performance testing including resources to be tested, test purpose, requested test environment, impacts to operations and expected results. This evaluation includes confirmation and review of the performance test tool and evaluation of LSM personnel resources to determine the ability of the system and site test teams to respond to specific testing requests.

This test sequence guides the reviewer in inspecting site (including GSFC) capability for performing, analyzing and reporting on short and long term performance trend analyses of site operational status, specific resource performance and maintenance activities. The LSM's performance management team procedures for monitoring site hardware and software to determine their operational states (on-line, failed, in maintenance mode, test mode, or simulation mode) are inspected.

Configuration: The subsystem needed to perform this sequence of tests are as follows. CSS/MSS, DSS, INS, ISS, & PLS. Refer to Appendix D for additional detail.

External Interfaces: The external interfaces (i.e. other ECS sites and data sources) needed for this sequence (both real and simulated) are listed:

SMC

EBnet

Operator Position(s): The operator positions from the ECS Maintenance and Operations Position Descriptions document needed to support this sequence are listed:

DAAC Production Planner

DAAC Resource Manager

Operational Scenario(s): The operations scenarios, taken from the Operations Scenarios for the ECS Project: Release-A document, that were used to develop tests in this sequence of tests are listed:

Resource Planning (Section 3.7.1) - A080520.010$G

User Notes Performance Degradation (Section 3.5.2) - A080530.010$G

Performance Trending Scenario (Section 3.5.4) - A080530.010$G

Preparing for New Algorithm Scenario (Section 3.5.3) - A080530.010$G

Test Dependencies: The following table identifies the test procedure(s) for this sequence of test that should be run prior to or concurrently with this test procedure.

Test Procedure No.	Site/Procedure No.	Comments
A080520.010$G	Software Development Benchmark Test	Prior
A080520.010$G	SMC/A080520.010$S	Concurrent
A080530.010$G	GSFC/A080520.010$G	Concurrent

8.5.2.1 Performance Testing

TEST Procedure No.: A080520.010$G	**Date Executed:**	**Test Conductor:**
Title:	Performance Testing	
Objective:	This test case verifies that the LSM has the capability to generate and coordinate requests for performance and benchmark testing. It also evaluates the LSM's ability to respond to testing requests.	

Requirements	Acceptance Criteria
EOSD0560#A	This requirement is verified through demonstration. **(RTM: test)** ECS benchmark tests and test data sets shall be defined for system verification and data quality evaluation. The benchmark tests and test data sets provided by a representative ECS element (e.g., a Data Server subsystem) will run to completion and generate reports.
EOSD0700#A	This requirement is verified through demonstration. Each ECS element shall provide the following, to be used in the revalidation of its functional performance: a. Benchmark test(s) b. Standard test data sets. A representative ECS element's (e.g., a Data Server subsystem) benchmark tests used to revalidate its functional performance will be run to completion.
EOSD0720#A	This requirement is verified through demonstration**.** Each ECS element shall be able to validate at any time during the life-time of the ECS that the ECS element primary functional performance is consistent with pre-defined operational benchmark tests. A representative ECS element's (e.g., a Data Server subsystem) benchmark tests will be run to completion.
SMC-3397#A	This requirement is verified through demonstration. **(RTM: test)**. The LSM shall generate, as needed, requests for performance testing, including, at a minimum: a. Resource to be tested b. Test purpose

	c. Requested test priority d. Required test environment e. Impacts to operations f. Expected test results Performance tools will be used by an operations staff to request performance testing which includes the following information: a. Resource to be tested b. Test purpose c. Requested test priority d. Required test environment e. Impacts to operations f. Expected test results

Test Inputs: Test case inputs include benchmark tests and standard test data sets for a representative ECS element (e.g., Data Server Subsystem) provided by the software development group. Scripts or M&O procedures to cause performance testing requests to be generated will also be needed.

Data Set Name	Data Set ID	File Name	Description	Version

Step-By-Step Procedures		
Step No.	**Input Action / Expected Results**	**Pass / Fail / Comments**
10	DAAC Production Planner: Follows M&O's to be developed procedure for requesting performance test (in this case, benchmark test).	
20	Expected Result: Performance test request procedure executed.	
30	DAAC Production Planner: Starts Resource Planning tool.	
40	Expected Result: Resource Planning window appears on the screen.	
50	DAAC Production Planner: Clicks Edit pushbutton on the Resource Planning window.	
60	Expected Result: Resource Request form appears in the window.	
70	DAAC Production Planner: Enters a request to run a benchmark test on GSFC DAAC host, including start and end times, resources, brief description including test purpose and priority, comments including required environment, impacts to operations, and expected test results. Then clicks "Accept".	
80	Expected Result: The request is entered into the resource planning database.	
90	DAAC Production Planner: Clicks Review pushbutton on the Resource Planning window.	
100	Expected Result: A list of resource requests appears on the screen.	
110	DAAC Production Planner: Double clicks on the request.	
120	Expected Result: The complete request as previously entered by the DAAC Production Planner appears on the screen.	
130	DAAC Production Planner: Inspects the request for validity. Clicks on the Validate and Approve pushbuttons on the screen.	
140	Expected Result: The resource request includes the "Validated" and "Approved" indicators.	
150	DAAC Production Planner: Clicks on the Accept pushbutton.	
160	Expected Result: The resource planning database is successfully updated.	
170	DAAC Production Planner: Initiates the GSFC DAAC performance benchmark test.	
180	Expected Result: The GSFC DAAC performance benchmark test runs to completion, storing a summary of results in the performance management database and printing a summary of the results.	

Data Reduction and Analysis Steps:	
The printed benchmark summaries are examined to ensure that they are consistent with the observations of the AT team during the actual test runs. The history log is analyzed and the performance benchmark test should include: a. Resource to be tested b. Test purpose c. Requested test priority d. Required test environment e. Impacts to operations f. Expected test results	
Signature:	**Date:**

8.5.2.2 Performance Monitoring and Analysis

TEST Procedure No.: A080530.010$G	**Date Executed:**	**Test Conductor:**

Title:	Performance Monitoring and Analysis
Objective:	This test case verifies the capabilities of the LSM to use performance management tools to augment overall system management activities for all GSFC DAAC resources and personnel. The test objectives are to observe and acquire performance trend information. Visualization capabilities that enable SMC and LSM operations personnel to determine the state for each principal node of the ECS network and the LAN, respectively, are confirmed. The DAAC-specific load and throughput performance analysis are conducted. The analysis determines if the DAAC exhibits a maximum steady state throughput at which some resource, e.g., CPU execution time, channel transfer rates, disc access rates, or memory, is fully occupied.

Requirements	Acceptance Criteria
DADS1340#A	This requirement is verified through demonstration. **(RTM: test.)** Each DADS shall use tools to analyze system performance. Tools such as HP OpenView, Spreadsheet application, Resource Planning will be used throughout the test to demonstrate that tools are used to analyze system performance.
DADS1360#A	This requirement is verified through test. Each DADS shall monitor the status of all storage systems used. The status of storage systems will be monitored by querying the management database.
DADS1620#A	This requirement is verified through demonstration. At each DADS tools shall be available for operations/systems/maintenance personnel to monitor performance. Tools such as HP OpenView, Spreadsheet application, Resource Planning will be used throughout the test to demonstrate that tools are used to monitor performance.
ESN-1060#A	This requirement is verified through test. The ESN performance management function shall provide the capability to evaluate the performance of ESN resources and interconnection activities. On ESDIS List.
ESN-1065#A	This requirement is verified through analysis. The ESN performance management function shall include trend analysis for prediction of loading and bottlenecks/delays. The trend analysis on ESN performance management function will include the prediction of loading and bottlenecks/delays. On ESDIS List.
NI-0460#A	This requirement is verified through test. ECS shall have the capability to receive periodic information regarding EBnet network performance and link utilization. The EBnet network performance and link utilization will be sent to ECS periodically and will be monitored by querying the management database and included in a performance report.

NSI-0060#A	This requirement is verified through test. (**RTM: blank)** NSI shall provide ECS SMC with load analysis reports, reflecting or summarizing NSI performance measurements over various time intervals. SMC will receive the load analysis reports from NSI and a trend analysis with various time intervals will be performed based on the NSI's load reports.
SMC-3305#A	This requirement is verified through test. The LSM shall monitor its elements hardware, and scientific and system software status to determine their operational states including, at a minimum : a. On-line b. Failed c. In maintenance d. In test mode e. In simulation mode The operational states (i.e., on-line, failed, in maintenance, in test mode and in simulation mode) of GSFC DAAC hardware, scientific and system software will be indicated via HP Open View.
SMC-3315#A	This requirement is verified through demonstration. The LSM shall monitor its elements schedule and execution of events. LSM will check the status of an executed task which is planned via the resource planning tool.
SMC-3325#A	This requirement is verified through demonstration. The LSM shall monitor execution of ground operations events. The performance data resulting from one of the ground operation events (i.e., performance testing: A080520.010$G, SMC-3397#A) will be collected and analyzed.
SMC-3335#A	This requirement is verified through test. The LSM shall compare and evaluate its elements actual schedule performance against planned schedule performance. A set of tasks will be executed and reports generated by LSM and the actual schedule performances will be manually compared against those of planned schedule performances.
SMC-3415#A	This requirement is verified through test. The LSM shall perform short and long-term trend analysis of element performance, including, at a minimum: a. Operational status b. Performance of a particular resource c. Maintenance activities (e.g., number of repairs per item) Graphical Performance trend analysis reports on operational status, performance and maintenance activities for a particular device (e.g., archive storage device) will be obtained and analyzed.

Test Inputs: A script that performs a query of the management database will be needed.

Data Set Name	Data Set ID	File Name	Description	Version

Step-By-Step Procedures		
Step No.	**Input Action / Expected Results**	**Pass / Fail / Comments**
10	DAAC Resource Manager: Initializes HP OpenView.	
20	Expected Result: The HP OpenView window appears displaying the root map for the system.	
30	DAAC resource manager: Follows procedure to place computer running Science Data Server (SDS) at GSFC DAAC in maintenance mode.	
40	Expected Result: The Science Data Server (SDS) host at GSFC DAAC is now in maintenance mode.	
50	DAAC resource manager: Uses the "Locate" function on the HP OpenView menu to bring up the map containing the Science Data Server (SDS) managed host at GSFC DAAC.	
60	Expected Result: The map containing the Science Data Server (SDS) managed host at GSFC DAAC appears on the screen. The host icon indicates that the host is in maintenance mode.	
70	DAAC resource manager: Follows procedure to place computer running Science Data Server (SDS) host at GSFC DAAC in test mode.	
80	Expected Result: The Science Data Server (SDS)host at GSFC DAAC is now in test mode.	
90	DAAC resource manager: Uses the "Locate" function on the HP OpenView menu to bring up the map containing the Science Data Server (SDS) managed host at GSFC DAAC.	
100	Expected Result: The map containing the Science Data Server (SDS) managed host at GSFC DAAC appears on the screen. The host icon indicates that the host is in test mode.	
110	DAAC resource manager: Follows procedure to place computer running Science Data Server (SDS) host at GSFC DAAC in simulation mode.	
120	Expected Result: The Science Data Server (SDS)host at GSFC DAAC is now in simulation mode.	
130	DAAC resource manager: Uses the "Locate" function on the HP OpenView menu to bring up the map containing the Science Data Server (SDS) managed host at GSFC DAAC.	
140	Expected Result: The map containing the Science Data Server (SDS) managed host at GSFC DAAC appears on the screen. The host icon indicates that the host is in simulation mode.	
150	DAAC resource manager: Places the host running the Science Data Server (SDS) at GSFC DAAC online.	
160	Expected Result: The host icon is green indicating that the host is up and functioning.	
170	DAAC Resource Manager: Induces a failure in a tape drive. (Possibly, attempt to write to a write protected tape cartridge.)	

180	Expected Result: Failure status for the tape drive appears.	
190	DAAC Resource Manager: Clicks on the icon for the host to which the tape drive is connected.	
200	Expected Result: The icon is highlighted.	
210	DAAC Resource Manager: Requests to view status of host hardware.	
220	Expected Result: The status display indicates failure status for the tape drive.	
230	DAAC Resource Manager: Runs a script that performs a query of the management database for status and performance information on storage systems, network utilization, ground operation events (e.g., performance testing) etc. The script will create a report from the data.	
240	Expected Result: A report containing the desired status and performance information is printed. It is saved for post test analysis.	
250	DAAC Resource Manager: Starts up the spreadsheet application.	
260	Expected Result: The spreadsheet is up and running.	
270	DAAC Resource Manager: Imports the monthly network performance data into the spreadsheet.	
280	Expected Result: The network performance data from the management database appear in the spreadsheet cells.	
290	DAAC Resource Manager: Creates spreadsheet tables (using the spreadsheet package) containing the network performance data.	
300	expected Result: The spreadsheet tables containing the network performance data are created.	
310	DAAC Resource Manager: Enters spreadsheet command to create weekly trend predictions for the next six months for the network performance values using statistical trending functions provided in the spreadsheet application.	
320	Expected Result: The spreadsheet application calculates future values for the performance metrics using statistical trending functions provided as part of the spreadsheet package.	
330	DAAC Resource Manager: Enters spreadsheet commands to create graphical prepresentations of the trend predictions created in the previous step .	
340	Expected Result: The spreadsheet application creates a line graph depicting both the actual data stored in the management database and the future values predicted by the spreadsheet for each of the network performance metrics.	
350	DAAC Resource Manager: Change the time interval to be used in trend analysis to get the short term trend analysis.	
360	Expected Result: The graphs will be automatically updated to reflect the change in data.	
370	DAAC Resource Manager: At the conclusion of the performance test (A080520.010$G), enter HP OpenView command to view system performance data from the test.	
380	Expected Result: The performance data are displayed on the screen.	

390	DAAC Resource Manager: Retrieves from the management database performance data from a previous run of the same data.	
400	Expected Result: The previous performance test data are displayed on the screen.	
410	DAAC Resource Manager: Enters command to print a summary report of performance data from the two performance test runs.	
420	Expected Result: The summary report is printed. The results are used for post test analysis to determine the necessity of modifying or potential enhancements to system.	
Data Reduction and Analysis Steps: Spreadsheet tables containing the network performance data are printed and compared with the report generated by querying the management database. (Spreadsheet graphs are also printed, assuming the spreadsheet is capable of printing graph.) The site history log is printed and is examined to verify that the status changes and failures that occur during this test are recorded.		
Signature:		**Date:**

8.6 Ancillary Services Scenario

This scenario takes site management personnel through a series of cases involving the use of system services in the management of the site. It carries the site management staff through certain system fault detection and isolation instances, security monitoring episodes, and accounting and report generation sequences. AT of fault management activity evaluates the capability for performing site-level fault analysis, fault diagnostic testing and recovery actions. Evaluation of ECS accounting and accountability activities extends to LSM in-site functions including related data collection, analysis and reporting activities is assessed. Evaluation of ECS report generation capabilities extends to evaluating the capability for providing required reports specified by all of the services referenced in the system management scenario group.

8.6.1 Fault Management Sequence

This sequence confirms the ECS capability to detect site-level faults and to analyze fault conditions, perform diagnostic testing, correct and recover from faults (or execute suitable contingency actions). The site operations teams confirm each site's capability to recover from global faults such as system failures, global data losses, or catastrophic security violations as well as local fault conditions. The GSFC DAAC operation personnel capabilities and test tools for isolating, locating, identifying and analyzing faults at the system and site level (except for flight operations faults) are confirmed by inspection of training records and by evaluation of operator performance during abnormal shutdown and recovery demonstrations (Sections 8.1.4 and 8.1.5). The GSFC DAAC capabilities for performing fault diagnostic testing are confirmed. The GSFC DAAC capability for recovering from fault situations is evaluated during previous shutdown and recovery testing.

Configuration: The subsystem needed to perform this sequence of tests are as follows. CSS/MSS, DSS, INS, ISS, & PLS. Refer to Appendix D for additional detail.

External Interfaces: The external interfaces (i.e. other ECS sites and data sources) needed for this sequence (both real and simulated) are listed:

SMC

EOC

LaRC ECS DAAC

EDC ECS DAAC

Operator Position(s): The operator positions from the ECS Maintenance and Operations Position Descriptions document (607/OP2) needed to support this sequence are listed:

DAAC Computer Operator

DAAC Resource Manager

DAAC Operations Supervisor

DAAC User Services Representative

TT Review Board

Operational Scenario(s): The operations scenarios, taken from the Operations Scenarios for the ECS Project: Release-A document, that were used to develop tests in this sequence of tests are listed:

Trouble Ticket and Problem Tracking Scenario (Section 3.2.1)

Non Conformance Report Scenario (Section 3.14.5)

Test Dependencies: There are no test dependencies needed for this sequence of tests.

8.6.1.1 Data Archive and Distribution Fault Analysis and Diagnostic Testing

TEST Procedure No.: A080610.020$G	**Date Executed:**	**Test Conductor:**
Title:	Data Archive and Distribution Fault Analysis and Diagnostic Testing	
Objective:	This test verifies the fault management requirements for the disk archive and distribution subsystem of the ECS. Simulated faults are induced in the subsystem to verify fault detection, fault isolation and reporting.	

Requirements	Acceptance Criteria
DADS0901#A	This requirement is verified through test. The DADS element shall collect the management data used to support the following system management functions: a. Fault Management b. Configuration Management d. Accountability Management e. Performance Management f. Security Management g. Scheduling Management h. Distribution and Ingest Management

	A storage media fault induced into the DSS must be properly managed such that the fault is detected, system operators are notified about the fault, and the fault is logged and forwarded to the SMC. The test does not include DADS0901#1 items b through h.
DADS1300#A	This requirement is verified through test. Each DADS shall display all faults to the system operators. A storage media fault induced into the DSS must be detected and displayed to the system operators.
DADS1310#A	This requirement is verified through test. Each DADS shall track and report to the SMC problems such as missing or corrupted files requiring restoration or regeneration of data. A missing file fault induced into the DSS must be detected, logged and reported to the SMC.
DADS1320#A	This requirement is verified through test. Each DADS shall provide to the SMC fault isolation information at the DADS system and subsystem levels. The DSS must report the failed device name or media, failure code or reason and the time/date of the failure to the SMC for all induced DSS faults.
DADS1330#A	This requirement is verified through test. Each DADS shall provide information to support fault isolation between the DADS and other ECS-unique elements and external interfaces to the LSM. A fault induced during a science software package delivery must be reported in the Error Log with sufficient information included to support isolation of the fault..
EOSD0730#A	This requirement is verified through test. Each ECS element shall be capable of verifying the fidelity of the ECS element interface to: a. Other ECS elements at any time during the lifetime of the ECS b. Entities external to ECS at any time during the lifetime of the ECS The MSS must be able to accurately depict the operational status of all ECS elements and update this status following simulated faults including a storage media fault, missing file fault, and DADS interface fault.
IMS-1620#A	This requirement is verified through test. The IMS element shall collect the management data used to support the following system management functions: a. Fault Management b. Configuration Management d. Accountability Management e. Performance Management f. Security Management g. Scheduling Management. A storage media fault induced into the DSS must be properly managed such that the fault is detected, system operators are notified about the fault, and the fault is logged and forwarded to the SMC. The test does not include IMS-1620#A items b through g.
IMS-1760#A	This requirement is verified through demonstration. The IMS shall send detected hardware faults to the SMC, to include at a minimum: a. IMS processors b. IMS network interfaces

	c. Storage devices Simulated faults including a storage media fault, missing file fault, and DADS interface fault must be properly managed such that the fault is detected, system operators are notified about the fault, and the fault is logged and forwarded to the SMC.
NI-0430#A	This requirement is verified through test. ECS shall have the capability to receive notification of faults in the NOLAN network that may affect the quality of NOLAN services between ECS and its users. Simulated faults including a storage media fault, missing file fault, and DADS interface fault must be properly managed such that the fault is detected, system operators are notified about the fault, and the fault is logged and forwarded to the SMC.
NI-0440#A	This requirement is verified through test. ECS shall have the capability to receive information regarding fault status and estimated time to repair or resolve NOLAN faults that may affect the quality of NOLAN services between ECS and its users. Simulated faults including a storage media fault, missing file fault, and DADS interface fault must be properly managed such that the fault is detected, system operators are notified about the fault, and the fault is logged and forwarded to the SMC.
NI-0450#A	This requirement is verified through test. ECS shall have the capability to receive periodic summary information about faults that may have affected the quality of NOLAN services between ECS and its users. Simulated faults including a storage media fault, missing file fault, and DADS interface fault must be properly managed such that the fault is detected, system operators are notified about the fault, and the fault is logged and forwarded to the SMC.
NI-0470#A	This requirement is verified through test. ECS shall have the capability to receive notifications of security breaches at NOLAN sites or within the NOLAN network that could potentially affect ECS sites.
NI-0480#A	This requirement is verified through test. ECS shall have the capability to send to NOLAN notifications of security breaches at ECS facilities that could affect NOLAN and other EOSDIS sites. Simulated faults including a storage media fault, missing file fault, and DADS interface fault must be properly managed such that the fault is detected, system operators are notified about the fault, and the fault is logged and forwarded to the SMC.
SMC-4315#A	This requirement is verified through test. The LSM shall, at a minimum, isolate, locate, and identify faults, identify subsystem, equipment, and software faults, and identify the nature of the faults within its element. The MSS must be able to accurately depict the operational status of all ECS elements and update this status following simulated faults including a storage media fault, missing file fault, DADS interface fault, and data processing fault.
SMC-4325#A	This requirement is verified through demonstration. The LSM shall request fault diagnosis testing be performed, including, at a minimum: a. Software and hardware tolerance testing

	b. Resource-to-resource connectivity testing within its element The MSS Fault Management Application Service must correctly fault isolate a storage media fault, missing file fault, DADS interface fault, and data processing fault.
SMC-4335#A	This requirement is verified through test. The LSM shall generate fault recovery commands, directives, and instructions within its element. The MSS Fault Management Application Service must provide instructions for returning the failing resources to service.

Step-By-Step Procedures		
Step No.	**Input Action / Expected Results**	**Pass / Fail / Comments**
Storage Media Fault Test		
10	Resource Manager: Login to the DAAC MSS server workstation using a valid ID and password as an administrator.	
20	Expected Results: Access to the DAAC MSS server is available.	
30	Resource Manager: Initialize HP OpenView using the <ovw &> command.	
40	Expected Results: A map depicting the overall topology is displayed.	
50	Resource Manager: Double click on the 'GSFC' icon to bring up the GSFC window.	
60	Expected Results: The GSFC submap is displayed on the screen.	
70	Resource Manager: Select 'Options" form the menu bar, followed by 'Topology/Status Polling : IP..."	
80	Expected Results: A map depicting the site configuration is accurately displayed. All icon symbols are on-line, displayed in green.	
90	Resource Manager: Simulate a device failure by taking the APC Server RAID storage device off-line.	
100	Expected Results: The icon for the RAID storage device is red and the GSFC icon is yellow.	
110	Resource Manager: Double click on **Diagnose, Network Activity, Demand Poll**.	
120	Expected Results: Hardware polling is initiated.	
130	Resource Manager: Double click on the red RAID storage device icon.	
140	Expected Results: Node submap opens with RAID storage interface red.	
150	Resource Manager: Place the APC Server RAID storage device back on-line.	
160	Expected Results: Submap icons are green.	
170	Resource Manager: Open the **Event Categories** window.	
180	Expected Results: The **Event Categories** window is displayed on the screen.	
190	Resource Manager: Select **Error Events** from the list of event categories.	
200	Expected Results: The **Event Browser** window displays a list of error events.	
210	Resource Manager: Verify the **Event Browser** displays the proper information in accordance with the Data Reduction and Analysis Steps A through C.	

220	Expected Results: The **Event Browser** displays the proper information in accordance with the Data Reduction and Analysis Steps A through C.	
230	Operations Supervisor: Login to the MSS server workstation using a valid ID and password as an administrator.	
240	Expected Results: Access to the MSS server is available.	
250	Operations Supervisor: Initialize HP OpenView using the <ovw &> command.	
260	Expected Result: The HP OpenView main menu is displayed on the screen depicting a map of the overall topology.	
270	Operations Supervisor: Double click on the 'GSFC' icon to bring up the GSFC window.	
280	Expected Results: The GSFC submap is displayed on the screen.	
290	Operations Supervisor: Open the **Event Categories** window	
300	Expected Results: The **Event Categories** window is displayed on the screen.	
310	Operations Supervisor: Select **Error Events** from the list of event categories.	
320	Expected Results: The **Event Browser** window displays a list of error events.	
330	Operations Supervisor: Verify the **Event Browser** displays the proper information in accordance with the Data Reduction and Analysis Steps A through C.	
340	Expected Results: The **Event Browser** displays the proper information in accordance with the Data Reduction and Analysis Steps A through C.	
350	Operations Supervisor: Exits HP OpenView.	
360	Expected Results: The administrator main menu is displayed on the screen.	
Missing File Fault DADS1310#A		
370	Production Planner: Rename a file required by a science software package.	
380	Expected Results: The file is renamed.	
390	Production Planner: Submit the processing request to run the science algorithm.	
400	Expected Results: The science software halts with an error message identifying the missing data file.	
410	Production Planner: Initialize HP OpenView using the <ovw &> command.	
420	Expected Results: A map depicting the overall topology is displayed.	
430	Production Planner: Open the **Event Categories** window.	
440	Expected Results: The **Event Categories** window is displayed on the screen.	

450	Production Planner: Select **Application Alert Events** from the list of event categories.	
460	Expected Results: The **Event Browser** window displays a list of error events.	
470	Production Planner: Verify the **Event Browser** displays the proper information in accordance with the Data Reduction and Analysis Steps D through F.	
480	Expected Results: The **Event Browser** displays the proper information in accordance with the Data Reduction and Analysis Steps D through F.	
490	Operations Supervisor: Exits HP OpenView.	
500	Expected Results: The administrator main menu is displayed on the screen.	
DADS Interface Test		
510	Data Specialist: Initialize HP OpenView using the <OVW &> command.	
520	Expected Result: A map depicting the overall topology is displayed.	
530	Data Specialist: Double click on the 'GSFC' icon.	
540	Expected Result: A map depicting the GSFC configuration is accurately displayed with all symbols displayed in green (on-line).	
550	Data Specialist: Begin transfer of the Science Software Package.	
560	Expected Results: The Science Software Package is transferred.	
570	Data Specialist: Shutdown the local host.	
580	Expected Results: The file transfer is halted. The host symbol on the Open View GSFC map is red.	
590	Data Specialist: Examine the history log containing the fault report.	
600	Expected Results: The history log verifies the host fault and file transfer fault.	
Data Processing Fault Test		
610	Production Planner: Login to the DAAC MSS server workstation using a valid ID and password as an administrator.	
620	Expected Results: Access to the DAAC MSS server is available.	
630	Production Planner: Initialize HP OpenView using the <ovw &> command.	
640	Expected Result: A map depicting the overall topology is displayed.	
650	Production Planner: Double click on the 'GSFC' icon.	
660	Expected Result: A window for 'Imp' is displayed.	
670	Production Planner: Double click on the science data processing icon.	
680	Expected Result: A window for the science data processor is displayed.	

690	Production Planner: Login to the science data processor.	
700	Expected Results: Access to the science data processor.	
710	Production Planner: Activate the Autosys GUI using the **autosc &** command	
720	Expected Result: The Autosys GUI is displayed.	
730	Production Planner: Activate the Autosys Job Activity Console GUI using the **autocons &** command.	
740	Expected Result: The Autosys Job Control Panel is displayed.	
750	Production Planner: Click on the Job Definition button in the Control Panel.	
760	Expected Results: The Job Definition dialog box is displayed.	
770	Production Planner: Using the Job Definition dialog box, submit a job for execution.	
780	Expected Results: The job executes.	
790	Production Planner: Shutdown the science data processor.	
800	Expected Results: Execution of the science data processing job is stopped.	
810	Production Planner: Using HP OpenView, display system status.	
820	Expected Results: a. The icon for GSFC is red b. The icon for IP icon is red c. The icon for the science processor is red d. The fault is logged in the error log file	
830	Resource Controller: Login at the SMC MSS server workstation using a valid ID and password as an administrator.	
840	Expected Results: Access to the SMC MSS server is available.	
850	Resource Controller: Initialize HP OpenView using the <ovw &> command.	
860	Expected Results: A map depicting the overall topology is displayed. The GSFC icon is red.	
870	Resource Controller: Double click on the 'GSFC' icon.	
880	Expected Results: a. A window for 'IPMap' is displayed. b. The IP icon is red c. The icon for the GSFC science processor is red	
890	Resource Controller: Restart the science data processor.	

900	Expected Results: HP OpenView on the MSS Server indicates the following status: a. The icon for GSFC is red b. The icon for IP icon is red c. The icon for the science processor is red d. The fault is logged in the error log file	
910	Resource Controller: Check the status of science data processing jobs.	
920	Expected Result: The submitted science data processing job has a status of [JOB FAILURE].	

Data Reduction and Analysis Steps:

A. The following materials should be secured for analysis:
   1. Error Event Log Printout.

B. Search the list of error events to find the APC Server RAID storage device failure produced by this test.

C. Verify that the Event Browser provides the following information:
   1. Severity is critical
   2. Date/Time of the fault are correct
   3. Source identifies the APC Server RAID storage device
   4. An appropriate message identifies the fault

D. The following materials should be secured for analysis:
   1. Error Event Log Printout.

E. Search the list of error events to find the APC Server RAID storage device failure produced by this test.

F. Verify that the Event Browser provides the following information:
   1. Severity is critical
   2. Date/Time of the fault are correct
   3. Source identifies a science data processing fault
   4. An appropriate message identifies the fault

Signature:	**Date:**

8.6.1.2 Product Generation Fault Analysis and Diagnostics Testing

This test procedure is not applicable for the GSFC Volume of the Acceptance Test Procedures document for Release A.

8.6.1.3 Communications Fault Analysis and Diagnostics Testing

TEST Procedure No.:	**Date Executed:**	**Test Conductor:**
A080610.050$G		
Title:	Communications Fault Analysis and Diagnostic Testing	
Objective:	This test verifies the fault management requirements for the communications subsystem of the ECS. Simulated faults are induced in the subsystem to verify fault detection, fault isolation and reporting.	
Requirements	**Acceptance Criteria**	

ESN-0650#A	This requirement is verified through test. The ESN shall perform the following network management functions for each protocol stack implemented in any ECS element, and each communications facility: a. Network Configuration Management b. Network Fault Management c. Network Performance Management d. Network Security Management A CSS fault induced by interrupting a network connection must be properly managed such that the fault is detected, system operators are notified about the fault, and the fault is logged and forwarded to the SMC. This test does not include ESN-0650#A items a, c and d.
ESN-0740#A	This requirement is verified by test. The ESN network management service shall retrieve performance/fault data about ESN protocol stacks and equipment. A CSS fault induced by interrupting a network connection must be detected and information provided that accurately identifies the fault. Performance data is not tested in this test case.
ESN-0810#A	This requirement is verified through test. ESN shall provide the following fault management functions at a minimum: a. detect the occurrence of faults, b. control the collection of fault information, and c. diagnose the probable cause of a detected fault A CSS fault induced by interrupting a network connection must be detected, accurately diagnosed, and logged.
ESN-0815#A	This requirement is verified through analysis. Network simulation and traffic modeling capability shall be provided to troubleshoot network problems and to use in network planning. The Tester uses network simulation to solve the network fault.
ESN-0830#A	This requirement is verified through test. The ESN shall have the capability to detect and report communications related errors and events both locally and at the ESN network management facility. An ISS fault induced by interrupting a network connection must be detected, accurately diagnosed, logged and reported locally and at the SMC.
ESN-0840#A	This requirement is verified through test. The ESN shall have error reporting, event logging and generation of alerts. A CSS fault induced by interrupting a network connection must be reported and logged in the event log file and alerts generated.
ESN-0900#A	This requirement is verified through test. Errors and events to be detected shall include at least: a. communications software version or configuration errors b. communications hardware errors c. protocol errors d. performance degradation conditions e. telecommunications errors and failures CSS faults induced by interrupting a telecommunication connection, network connection, or configuration error must be reported and logged in the event log file and alerts generated. This test does not test item d of the requirement
ESN-0910#A	This requirement is verified through test.

	The ESN fault management shall provide the capability to perform the following functions, at a minimum, both locally and at the ESN network management facility: a. set, view, and change alert threshold values b. enable and disable alert notifications (alarms) within a system c. enable and disable event reports within a system d. manage error and event logging files The MSS Monitor/Control Service will be used to set fault thresholds, enable/disable alarms and reports caused by CSS faults and schedule the transfer of fault management data to the SMC.
ESN-0920#A	This requirement is verified through inspection. The ESN shall provide a set of utilities to perform diagnostic and testing functions for purposes of fault isolation. The MSS Fault Management Application Service will provide utilities to perform diagnostics and testing of connectivity between ECS hosts and router, the ability to reach hosts and routers, and the availability of network services at hosts.
ESN-1000#A	This requirement is verified through demonstration. The ESN network management function shall have the capability to build histories for different types of errors and events, and the capability to analyze errors and recommend corrective action wherever practical. The MSS Fault Management Application Service will demonstrate the ability to build histories for different types of errors and events detected, for the purpose of analysis.
ESN-1010#A	This requirement is verified through test. The ESN shall provide, for selective use as a debugging aid, the capability to perform packet tracing of its supported protocols. This requirement is verified during Integration and Test and is not verified during this test.
NSI-0030#A	This requirement is verified through test. NSI shall have the capability of sending and ECS shall have the capability of receiving notification of faults in NSI's network that may affect the quality of NSI services between ECS and its users. The Tester will send a fault notification message across the NSI.
NSI-0040#A	This requirement is verified through test. NSI shall make available to ECS information regarding fault status and estimated time to repair or resolve NSI faults that may affect the quality of NSI services between ECS and its users. The MSS will receive notification of NSI faults.
NSI-0050#A	This requirement is verified through test. NSI shall provide ECS with periodic summary information about faults that may have affected the quality of NSI services between ECS and its users. The MSS will receive periodic summary information about NSI faults.

Step-By-Step Procedures		
Step No.	**Input Action / Expected Results**	**Pass / Fail / Comments**
Communications Hardware Fault		
10	Computer Operator: Logon the MSS server workstation.	
15	Expected Results: MSS server workstation is available.	
20	Computer Operator: Initialize HP OpenView using the <ovw &> command.	
30	Expected Results: A map depicting the overall topology is displayed.	
40	Computer Operator: Double click on the GSFC icon.	
50	Expected Results: A map depicting the GSFC DAAC configuration is accurately displayed with all symbols displayed in green.	
60	Computer Operator: Prepare to send an EMAIL message of considerable length (20 pages or more) to another DAAC.	
70	Tester: Instruct the Computer Operator to send the EMAIL message, wait approximately 2 seconds then remove power from the FDDI concentrator.	
80	Expected Results: a. The FDD Concentrator symbol is red b. Audible alarm sounds c. The fault is logged in the error log file d. The fault is forwarded to the SMC	
90	Computer Operator: Double click on the red FDDI concentrator symbol.	
100	Expected Results: Information accurately describing the fault is displayed.	
110	Computer Operator: Close the window for the FDDI concentrator	
120	Tester: Restore power to the FDDI concentrator.	
130	Expected Results: The FDDI concentrator symbol is green.	
140	Computer Operator: Verify the fault is accurately logged and described in the error log file.	
Network Communications Fault		
150	Tester: Disconnect the LAN cable from the ingest server.	
160	Expected Results: a. The ingest server symbol is red b. Audible alarm sounds c. The fault is logged in the error log file d. The fault is forwarded to the SMC	
170	Computer Operator: Double click on the red ingest server symbol.	

180	Expected Results: Information accurately describing the fault is displayed.	
190	Computer Operator: Close the window for the ingest server.	
200	Tester: Restore the ingest server LAN connection.	
210	Expected Results: The ingest server symbol is green.	
220	Computer Operator: Verify the fault is accurately logged and described in the error log file.	
	Communication Configuration Fault	
230	Tester: Change the IP address of one data management server.	
240	Expected Results: a. The data management server symbol is red b. Audible alarm sounds c. The fault is logged in the error log file d. The fault is forwarded to the SMC	
250	Computer Operator: Double click on the red data management server symbol.	
260	Expected Results: Information accurately describing the fault is displayed.	
270	Computer Operator: Close the window for the data management server.	
280	Tester: Restore the data management server IP address.	
290	Expected Results: The data management server symbol is green.	
300	Computer Operator: Verify the fault is accurately logged and described in the error log file.	
	Histories	
310	Computer Operator: Initiate the MSS Fault Management Application Service.	
320	Expected Result: The MSS Fault Management Application Service appears on the screen.	
330	Computer Operator: Using the MSS Fault Management Application Service, build a history for all communications faults for today's date.	
340	Expected Results: The MSS Fault Management Application Service displays a history of all communications faults produced by this test.	
	Fault Management	
350	Computer Operator: Initiate the MSS Monitor/Control Service.	
360	Expected Result: The MSS Monitor/Control Service application appears on the screen.	
370	Computer Operator: Change threshold values managed resources.	
380	Expected Result: The MSS Monitor/Control Service accepts valid threshold value changes.	

390	Computer Operator: Change the enable/disable alert status of managed resources.	
400	Expected Result: The MSS Monitor/Control Service accepts changes to the enable/disable alert status of managed resources.	
410	Computer Operator: Exit the MSS Monitor/Control Service.	
420	Computer Operator: Initiate the MSS Fault Management Application Service.	
430	Expected Result: The MSS Fault Management Application Service appears on the screen.	
440	Computer Operator: Configure the application to display all fault categories.	
450	Expected Result: A list of all managed resources is displayed.	
460	Computer Operator: Change the enable/disable fault notification status of at least two managed resources.	
470	Expected Result: The MSS Fault Management Application Service accepts the changes.	
Data Reduction and Analysis Steps:		
Signature:		**Date:**

8.6.1.4 Trouble Ticketing

TEST Procedure No.: A080610.060$G	**Date Executed:**	**Test Conductor:**
Title: Trouble Ticketing		
Objective: This test verifies the ability to submit a trouble ticket.		

Requirements	**Acceptance Criteria**
SMC-8860#A	This requirement is verified through test. The SMC shall have the capability to generate detailed and summary fault management reports describing the fault management of ground resources, including, at a minimum: a. Fault type and description b. Time of occurrence of fault c. Effect on system d. Status of fault resolution e. Fault statistics The Trouble Ticketing Service must have a graphical user interface to support the entry and editing of trouble tickets.

Test Inputs:

Data Set Name	**Data Set ID**	**File Name**	**Description**	**Version**

Step-By-Step Procedures		
Step No.	**Input Action / Expected Results**	**Pass / Fail / Comments**
10	DAAC User Services Representative: Upon realization that a problem exists, selects the Trouble Ticket icon from the ECS Desktop.	
20	Expected Results: ECS Desktop invokes user-preferred browser with Trouble Ticketing home page URL.	
30	DAAC User Services Representative: Views Trouble Ticketing HTML home page options.	
40	Expected Results: Options: Submit TT, List TTs are displayed on the screen.	
50	DAAC User Services Representative: Selects the Submit Option.	
60	Expected Results: The system calls the Trouble Ticket Submit page. The system automatically retrieves user information from database. (e.g., e-mail address, name, phone number, etc.).	
70	DAAC User Services Representative: Enters problem impact, problem short description, and problem long description. When satisfied with the entry, clicks on the submit button to submit TT.	
80	Expected Results: The system creates new entry in Remedy, notifies Operations Supervisor, displays successful submission HTML page (except for internal submissions) which includes the TT number, and notifies User via e-mail which also includes the TT number.	
90	DAAC User Services Representative: Receives e-mail verifying that the TT was submitted.	
100	Expected Results: An e-mail message receipt notification pop-up window is displayed on the screen. The system notifies the Operations Supervisor of the new Trouble Ticket.	
110	Operations Supervisor: Refreshes TT list to check for most recent TTs.	
120	Expected Results: The system (Remedy) refreshes list.	
130	Operations Supervisor: Selects TT for work and opens it.	
140	Expected Results: The system (Remedy) opens TT.	
150	Operations Supervisor: On examining the detailed information, changes the value of Ticket Status from New to Assigned.	
160	Expected Results: The system displays the Options: Assigned, Forwarded.	
170	Operations Supervisor: Assigns the value of Low to the Assigned-Priority field.	
180	Expected Results: The system displays the Options: Low, Medium, High)	
190	Operations Supervisor: Assigns the Trouble Ticket to a particular Computer Operator to fix the problem and clicks on **Apply** to carry out these new changes.	

200	Expected Results: The system (Remedy) delivers e-mail to the Computer Operator.	
210	Computer Operator: Receives e-mail notifying him/her of the assignment.	
220	Expected Results: An e-mail message receipt notification pop-up window is displayed on the screen.	
230	Computer Operator: Inputs an initial entry into the Resolution Log (which is a free text diary) indicating the proposed course of action.	
240	Expected Results: The Resolution Log displays the initial entry.	
250	Computer Operator: Then clicks on **Apply** to update the TT with this status.	
260	Expected Results: The system (Remedy) updates TT.	
270	Computer Operator: Analyzes and attempts to resolve the issue that the TT addresses, then updates the Resolution Log with pertinent information. Each update to the Resolution Log is followed by a click on the Apply button to commit the update.	
280	Expected Results: The system (Remedy) updates Resolution Log with time/date, name of modifier and current log.	
290	Computer Operator: After finding a solution, changes the Ticket Status to **Solution Proposed**	
300	Expected Results: The system displays the Options: Solution Proposed.	
310	TT Review Board: Compiles a package of new "Solution Proposed" TTs for review by the board. Considers the sensibility and long term effects of the proposed solution for this TT. Approves the solution and changes the Status to **Implement Solution**.	
320	Expected Results: Options: Forwarded, Closed, Implement Solution are displayed on the screen.	
330	Computer Operator: Fixes the problem and changes Status to **Solution Implemented**.	
340	Expected Results: The problem is corrected and the new status displayed on the screen is **Solution Implemented**.	
350	TT Review Board: Approves fix select **Key Words**, **Closing Code**, **Hardware Resource**, and/or **Software Resource** values as applicable, and upon User Verification Closes TT.	
360	Expected Results: The trouble ticket is closed.	
370	Computer Operator: Sends e-mail to the DAAC User Services Representative notifying him/her of the TT being closed.	
380	Expected Results: An e-mail message receipt notification pop-up window is displayed on the screen.	
Data Reduction and Analysis Steps:		
Signature:		**Date:**

8.6.1.5 Non Conformance Report

TEST Procedure No.: A080610.070$S	**Date Executed:**	**Test Conductor:**
Title: Non Conformance Report		
Objective: This test verifies the ability of recording and reporting of a software problem.		

Requirements	**Acceptance Criteria**
SMC-8860#A	This requirement is verified through test. The SMC shall have the capability to generate detailed and summary fault management reports describing the fault management of ground resources, including, at a minimum: a. Fault type and description b. Time of occurrence of fault c. Effect on system d. Status of fault resolution e. Fault statistics The Trouble Ticketing Service must have a graphical user interface to support the entry and editing of trouble tickets.

Test Inputs:

Data Set Name	Data Set ID	File Name	Description	Version

Step-By-Step Procedures		
Step No.	**Input Action / Expected Results**	**Pass / Fail / Comments**
10	DAAC User Services Representative: Takes a call (or E-mail) reporting a software defect and clicks on the Trouble Ticketing tool icon on his desktop.	
20	Expected Results: Trouble Ticketing application starts up.	
30	DAAC User Services Representative: Fills in items in Trouble Ticket (e.g., application, platform, version, description, user information and E-mail address etc.) based on User's inputs. Rep confirms items with user, and submits ticket. For E-mail correspondence, a message is sent to the user with this information.	
40	Expected Results: Application submits the ticket to Remedy.	
50	DAAC User Services Representative: Regularly monitors trouble ticket status and notifies user when problem is resolved.	
60	Expected Results: Application notifies user when resolution is implemented.	
Data Reduction and Analysis Steps:		
Signature:		**Date:**

8.6.2 Security Management Sequence

This sequence provides the guidance in verifying the LSM's capabilities for establishing and maintaining security management data bases and for site-level security activities. This sequence verifies the LSM site-level abilities related to physical security password management, operational security, data security, privileges, and security compromise mitigation. The presence of system-level services for access control, authentication of user credentials is confirmed. Countermeasures for security threats such as unauthorized modification of data, disclosure of authentication information, denial of authorized service, and impersonation of authentication information, are also confirmed. Authentication, access control, data integrity, and data confidentiality protection functions are confirmed and evaluated against system and site requirements. Event functions (detection, reporting, and logging) are demonstrated and confirmed by comparison with system and site requirements.

Configuration: The subsystem needed to perform this sequence of tests are as follows. CSS/MSS, DSS, INS, ISS, & PLS. Refer to Appendix D for additional detail.

External Interfaces: The external interface (i.e. other ECS sites and data sources) needed for this sequence (both real and simulated) is listed:

SMC

Operator Position(s): The operator positions from the ECS Maintenance and Operations Position Descriptions document (607/OP2) needed to support this sequence are listed:

DAAC Resource Manager

DAAC Computer Operator

Operational Scenario(s): The operations scenario, taken from the Operations Scenarios for the ECS Project: Release-A document (605/OP1), that was used to develop tests in this sequence of tests are listed:

Security Management Login Failure Scenario (Section 3.6.1)

Test Dependencies: There are no test dependencies needed for this sequence of tests.

8.6.2.1 SMC Security Functions

This test procedure is not applicable for the GSFC Volume of the Acceptance Test Procedures document for Release A.

8.6.2.2 LSM Security Functions

TEST Procedure No.: A080620.040$G	**Date Executed:**	**Test Conductor:**
Title:	LSM Security Functions	
Objective:	The objective of this test is to verify the LSM security functions; such as maintaining, authenticating, and monitoring user and device accesses and privileges; performing security testing that includes, password auditing and site internal access/privileges checking; performing compromise detection (e.g. virus or worm penetration); and performing risk detection and analyses.	

Requirements	Acceptance Criteria
DADS1085#A	This requirement is verified through test. Each DADS shall maintain a data access log. The Tester must be able to access the data access log.
EOSD2400#A	This requirement is verified through test. ECS shall provide multiple categories of data protection based on the sensitivity levels of ECS data, as defined in NHB 2410.9. The system must control access to archived data to prevent unauthorized access. The system must authenticate that the interactive user is authorized.
EOSD2510#A	This requirement is verified through demonstration. ECS elements shall maintain an audit trail of: a. All accesses to the element security controlled data b. Users/processes/elements requesting access to element security controlled data c. Data access/manipulation operations performed on security controlled data d. Date and time of access to security controlled data e. Unsuccessful access attempt to the element security controlled data by unauthorized users/elements/processes f. Detected computer system viruses and worms

	g. Actions taken to contain or destroy a virus The CSS Security service must provide the capability to log audit information into security logs whenever authentication and authorization services are used. The audit information must contain the following: a. Date and time of the event b. User name c. Type of event d. Success or failure of the event e. Origin of the request.
EOSD2550#A	This requirement is verified through test. The ECS elements shall limit use of master passwords or use of a single password for large organizations requiring access to a mix of security controlled and non-sensitive data. The System must require a unique user identification and password for each individual user.
EOSD2650#A	This requirement is verified through test. The LSM shall report detected security violations to the SMC. The LSM must contact the SMC in the event of a security violation via electronic mail or telephone.
EOSD2710#A	This requirement is verified through demonstration. ECS elements shall report all detected computer viruses and actions taken to the SMC. The System must provide virus detection services. The LSM must report detected security violations to the SMC.
ESN-0010#A	This requirement is verified through test. ESN shall provide the following standard services: a. Data Transfer and Management Services b. Electronic Messaging Service c. Remote Terminal Service d. Process to Process Communication Service e. Directory and User Access Control Service f. Network Management Service g. Network Security and Access Control Service h. Internetwork Interface Services i. Bulletin Board Service The Tester must verify the various LSM security functions. This test does NOT verify parts a, b, c, d, e, f, h, and i of the requirement.
ESN-0650#A	This requirement is verified through test. The ESN shall perform the following network management functions for each protocol stack implemented in any ECS element, and each communications facility: a. Network Configuration Management b. Network Fault Management c. Network Performance Management d. Network Security Management The CSS Security service must provide the capability to create/modify/delete user accounts and privileges in the security registry. The CSS Security service must provide the capability to define/modify/delete group information in the security registry. This test does NOT verify parts a, b and c of the requirement.
ESN-1360#A	This requirement is verified through test. The ESN shall control access of processes and users through an

	authentication and authorization service that meets GNMP standards. The authentication and authorization service must meet GNMP standards.
ESN-1380#A	This requirement is verified through test. The ESN shall provide countermeasures for the following security threats related to data communications: a. modification of data (i.e., manipulation) while in transit over the network b. disclosure of authentication information c. degradation in network or processing resource performance through denial of service attack d. Impersonation of authentication credentials or authorization privileges. The CSS Security service must provide an API to check the authorization privileges of principals to access/control services/resources. The CSS Security service must support the Data Encryption Standard (DES) to encrypt and decrypt data.
ESN-1400#A	This requirement is verified through test. The following security functions and services, at a minimum, shall be provided: a. authentication b. access (authorization) control c. data integrity d. data confidentiality. The CSS Security service must provide an API to check the authorization privileges of principals to access/control services/resources. The CSS Security service must support the Data Encryption Standard (DES) to encrypt and decrypt data.
ESN-1430#A	This requirement is verified through test. The ESN shall provide the following security event functions: a. Event detection b. Event reporting c. Event logging. CSS Event Logger Service must provide capability to record security event and history data to an application specific log file.
IMS-1665#A	This requirement is verified through demonstration. The IMS shall provide to the SMC, IMS services usage by each user (to include at a minimum user name, IMS service identification, date/time stamp, time expended, facilities used) for later reporting and determination of access patterns. The GTWAY CI must log Service requests. The GTWAY CI must log the termination or successful completion of service requests. The log must provide IMS services usage by each user (to include at a minimum user name, IMS service identification, date/time stamp, time expended, facilities used).
NSI-0070#A	This requirement is verified through test. NSI shall have the capability of sending and ECS shall have the capability of receiving notification of security breaches at NSI sites or within the NSI network that could potentially affect ECS sites. The Tester must receive NSI security breach notifications.
NSI-0080#A	This requirement is verified through test. ECS shall have the capability of sending and NSI shall have the capability of receiving notification of security breaches at ECS facilities that could affect NSI and other EOSDIS sites.

	The Tester must sent ECS security breach notifications to the NSI.
SMC-5335#A	This requirement is verified through test. The LSM shall perform security testing that includes, at a minimum, password auditing and element internal access/privileges checking. The MSS site Security Management Application Service must have the capability to perform the following types of security tests: a. password auditing b. file system integrity checking c. auditing of user privileges d. auditing of resource access control information.
SMC-5345#A	This requirement is verified through inspection. The LSM shall perform compromise (e.g., virus or worm penetration) risk analysis, and detection. The System must provide virus detection services.
SMC-5355#A	This requirement is verified through test. The LSM shall isolate the compromised area, detach the compromised input I/O, and the compromised areas output I/O until the compromise has been eliminated. The MSS site Security Management Application Service must, upon the detection of a compromise, isolate the compromised input I/O, and the compromised area's output I/O until the compromise has been eliminated.
SMC-5365#A	This requirement is verified through test. The LSM shall generate recovery actions in response to the detection of compromises. The MSS Security Management Application Service must provide office automation support tools to enable the generation of directives and instructions for recovery from detected security events.
SMC-6325#A	This requirement is verified through demonstration. The LSM shall perform, as needed, data and user audit trails within its element. The LSM must have the ability to perform data and user audit trails within its element.
Test Inputs: Authorized/Approved user id and password	

Step-By-Step Procedures		
Step No.	**Input Action / Expected Results**	**Pass / Fail / Comments**
10	Resource Manager: Verifies the existence of virus detection software.	
20	Expected Results: The virus detection software is installed and operational on the system.	
30	Computer Operator: Executes a security administrator logon.	
40	Expected Results: The system displays the security administrator main menu.	
50	Computer Operator: Performs create, change and delete commands to the security registry.	
60	Expected Results: User accounts are created, changed and deleted.	
70	Computer Operator: Verifies that the user accounts contain username, password, group and user identification code, login directory and command line interpreter.	
80	Expected Results: User accounts reflect create, change and delete commands entered by the Computer Operator.	
90	Computer Operator: Logs off.	
100	Expected Results: The system displays the logon screen.	
110	Computer Operator: Executes logon with user id.	
120	Expected Results: The system displays the main menu.	
130	Computer Operator: Performs, create, change and delete commands to the security registry.	
140	Expected Results: The user accounts are created, changed and deleted from the system.	
150	Computer Operator: Verify that modifications are reflected in the user accounts.	
100	Expected Results: User accounts reflect create, change and delete commands entered by the Computer Operator.	
110	Computer Operator: Logs off.	
115	Expected Results: The ECS login screen is displayed on the screen.	
120	Computer Operator: Using SATAN and CRACK, attempts to log in by guessing passwords. Repeat multiple times.	
130	Expected Results: The security management service detects the multiple events after the preestablished threshold has been crossed. The service sends notification of security alert to the Computer Operator.	
140	Computer Operator: Receives multiple security alerts. Begins investigation into cause of alerts by invoking the events browser (log) to retrieve the security events.	

150	Expected Results: Displays the requested events. The information must contain the following: a. Date and time of the event b. User name c. Type of event d. Success or failure of the event e. Origin of the request	
160	Computer Operator: Discovers that the login attempts on the multiple hosts originated from the same area.	
170	Computer Operator: Contacts the MIS manager at the location of the User (Hacker) who proceeds to have the issue investigated locally. Sends e-mail to all ECS sites informing them of the event and to explicitly deny access from this area.	
180	Computer Operator: Modifies the network security authorization databases to deny all incoming accesses from the host in question.	
190	1st Authorized/Approved User: Logs on to ECS using a valid user id and password.	
200	Expected Results: The user is able to log onto the system. The next user screen appears.	
210	Tester: Using a network analyzer, verifies that the password is not readable over the network.	
220	2nd Authorized/Approved User: Attempts to log on to ECS using the same valid user id and password used by the 1st Authorized/Approved User in step 190.	
230	Expected Results: The user is unable to log onto the system. A message indicating the user is already logged on is displayed.	
240	1st Authorized/Approved User: Compromises the data by deleting files.	
250	Expected Result: The system detects the compromise, isolates it, until it can be eliminated.	
260	Computer Operator: Discovers that the security violation compromise.	
270	Computer Operator: Using the Office Automation tools provided, generates instructions for recovery from the detected security event.	
Data Reduction and Analysis Steps:		
Signature:		**Date:**

8.6.3 Accounting and Accountability Sequence

This sequence guides the evaluator through and assessment of the ECS and GSFC capability to perform compliant accounting and accountability functions. The ECS ability to establish, maintain, and update data tracking systems to track data transport from ECS input to ECS output, and to allow statusing of all product-production activities is confirmed by inspection of outputs.

Configuration: The subsystem needed to perform this sequence of tests are as follows. CSS/MSS, DSS, INS, ISS, & PLS. Refer to Appendix D for additional detail.

External Interfaces: The following external interfaces (i.e. other ECS sites and data sources) needed for this sequence (both real and simulated) are listed below.

ECS Client

Operator Positions: The following operator positions are needed to support this sequence.

Computer Operator

Operational Scenario: The following scenarios, taken from the ECS Operations Concept for the ECS Project, Part 2A document, are used during this sequence of tests:

Network Data Distribution (Pull) Scenario (Nominal) Scenario (Section 3.11.2)

Accountability Management Create User Account Scenario (Section 3.6.2)

Test Dependencies: There are no test dependencies required.

8.6.3.1 Accountability: Data Tracking and Audit Trails

This test procedure is not applicable for the GSFC Volume of the Acceptance Test Procedures document for Release A.

8.6.3.2 LSM Data Tracking

TEST Procedure No.: A080630.030$G	**Date Executed:**	**Test Conductor:**
Title:	LSM Data Tracking	
Objective:	This procedure verifies the ECS's ability to manage user accounts, track production activities, and to manage the configuration of system HWCI and CSCI elements.	

Requirements	Acceptance Criteria
SMC-5325#A	This requirement is verified through test. The LSM shall promulgate, maintain, authenticate, and monitor user and device accesses and privileges. A new approved user account must be added to the system including all account attributes, privileges, resource access. Account information must be available for review and modification.
SMC-6315#A	This requirement is verified through demonstration. The LSM must perform, as needed, security audit trails within its element. The MSS MUI must display a log of all activities for a user account and access attempts.

SMC-6335#A	This requirement is verified through demonstration. The LSM shall perform, as needed, maintain and update a data tracking system that, at a minimum: a. Tracks data transport from element input to element output. b. Allows the status of all product-production activities to be determined. The ECS data tracking system must list data transport activities and provide status of all product-production activities.
SMC-6345#A	This requirement is verified through demonstration. The LSM shall, as needed, perform configuration accountability to include, at a minimum, the audit of hardware and software resources within its element. The MSS configuration management application service must identify a particular software element whose version varies from the operational baseline.

Step-By-Step Procedures		
Step No.	**Input Action / Expected Results**	**Pass / Fail / Comments**
User Accountability Test		
10	Computer Operator: Login to the MSS server workstation using a valid ID and password as an administrator.	
20	Expected Results: Access to the MSS Server is available.	
30	Computer Operator: Using the MSS Security Management Application Service GUI, create a user account with the following attributes: a. user name b. password c. group identification code d. user identification code e. login directory f. resource access privileges	
40	Expected Results: The new user account is accepted by the system.	
50	Tester: Login as a remote user using the user name and password created in step 30.	
60	Expected Result: The user is logged onto the ECS and the search and order tool appears on the users screen.	
70	Tester: Logoff as a remote user.	
80	Expected Results: The login screen appears.	
90	Tester: Attempt to remote login to the ECS using an invalid password.	
100	Expected Result: The login attempt is denied.	
110	Tester: Attempt to repeat step 90 five times.	
120	Expected Result: Attempts to login are limited to five tries.	
130	Computer Operator: Using the MSS accountability management service MUI, view the activities log associated with the new user.	
140	Expected Results: The log should show one login for the new user and five unsuccessful attempts to login.	
Configuration Accountability Test		
150	Computer Operator: Using the configuration management application service, view the configuration of controlled resources that comprise the site's operational baseline.	
160	Expected Results: There are no variations from the operational baseline.	
150	Tester: Remove a printer from the site configuration. Remove a software application from the site configuration.	
160	Expected Results: The configuration management application service identifies the variants from the site operational baseline.	

170	Tester: Re-install the printer in the site configuration. Re-install the removed software into the site configuration.	
180	Expected Results: The configuration management application service shows no variations from the site's operational baseline.	
190	Computer Operator: Logoff of the system.	
200	Expected Results: The UNIX prompt appears.	
Data Reduction and Analysis Steps:		
Signature:		**Date:**

8.6.4 Report Generation Sequence

This sequence guides the evaluator in assessing ECS capability for performing the GSFC report generation required for Release A. This report generator can produce standard or customized outputs for a full range of inputs, such as a functional allocation report giving the current allocation of ground segment functions; summary configuration status reports; summary training reports; hardware configuration, system and scientific software reports; spares and consumables reports; lists of proposed enhancements; detailed and summary reports indicating the overall performance of the ECS Maintainability Status Reports; product generation status reports; ground resources performance reports; user feedback analysis reports; fault management reports; and security compromise reports. The report generators at GSFC are evaluated through inspection of output products and comparison of the products against site reporting requirements.

Configuration: The subsystem needed to perform this sequence of tests are as follows. CSS/MSS, DSS, INS, ISS, & PLS. Refer to Appendix D for additional detail.

External Interfaces: The external interfaces (i.e. other ECS sites and data sources) needed for this sequence (both real and simulated) are listed :

SMC

Operator Position(s): The operator positions from the ECS Maintenance and Operations Position Descriptions document (607-CD-001-002) needed to support this sequence are listed:

DAAC Operations Supervisor

DAAC Production Monitor

DAAC Computer Operator

Operational Scenario(s): There are no operations scenarios taken from the Operations Scenarios for the ECS Project: Release-A, used during this sequence of tests.

Test Dependencies: The following table identifies the test procedure(s) in a sequence of tests that should be run prior to or concurrently with a sequence or test procedure.

Test Procedure No.	Site/Procedure No.	Comments
A080640.030$G	A080640.030$S	prior

8.6.4.1 SMC Report Generator

This test procedure is not applicable for the GSFC Volume of the Acceptance Test Procedures document for Release A.

8.6.4.2 LSM Report Generator

TEST Procedure No.: A080640.030$G	**Date Executed:**	**Test Conductor:**
Title: LSM Report Generator		
Objective: Demonstrate the existence and the capabilities of a site-specific report generator residing within the site configuration, and the capability to generate pre-defined reports.		

Requirements	Acceptance Criteria
SMC-8305#A	This requirement is verified through test. The LSM shall have the same report generator capability as for the SMC, except it shall be limited to generating reports covering only its particular site or its particular element. The Production Monitor-QA tests that the system provides the capability of a site report generator and that input data sets are available for report access.
SMC-8705#A	This requirement is verified through test. The LSM shall have the capability to generate the same types of reports listed under the SMC report generation service, except that each report covers only its particular site or its particular element. The Tester tests that the system provides the capability and use of a site report generator to produce standard reports.
SMC-8710#A	This requirement is tested at the SMC and is verified through test. The SMC shall have the capability to generate summary configuration status reports that includes, at a minimum: a. Current status of all hardware, system and scientific software b. Reason why an item is not currently operational. A report is generated with summary information showing the site inventory of hardware, system and scientific software, and spares and consumables. Information generated at the SMC will be accessed for use in this test procedure.
SMC-8750#A	This requirement is semi-automated at the SMC for this release, and is verified through analysis. The SMC shall have the capability to generate detailed and summary training reports, including, at a minimum: a. Training programs b. Training course schedules c. Training course contents d. Training course locations e. Training attendees A report is generated that has detailed and summary information on training programs, training course schedules, training course contents, training course locations, and training attendees. Information generated at the SMC will be accessed for use in this test

	procedure.
ESN-0760#A	This requirement is verified through test. The ESN report generation function shall provide, on an interactive and scheduled basis, accounting, network configuration, fault and performance management information. The Tester tests that the system provides the capability to report information concerning accounting, network configuration, and fault and performance management.
ESN-0770#A	This requirement is verified through test. The ESN query capability shall generate ad hoc statistics and reports based on parameters entered. The Tester tests that the system provides the capability and use of a site report generator to produce communication reports based on the entered parameters.
ESN-0775#A	This requirement is verified through test. The ESN management service shall have the capability to redirect its reports to different devices such as console, disk or printer. The Tester displays the steps involved in producing standard or customized reports through use of the site report generator, from user request through output to selected media.
SMC-8770#A	This requirement is satisfied at the SMC, and his requirement is verified through test. The SMC shall have the capability to generate, at a minimum, detailed and summary reports showing the inventory of: a. Hardware, system, and scientific software b. Spares and consumables A report is generated composed of summary information showing the site inventory of hardware, system and scientific software, and spares and consumables. Information generated at the SMC will be accessed for use in this test procedure.
SMC-8790#A	This requirement is satisfied at the SMC and this requirement is verified through analysis. The SMC shall have the capability to generate, as necessary, a list of proposed enhancements with at least these elements: a. Proposal name b. Description of enhancement c. Rationale d. Impacts e. Costs f. Milestone schedule A report is generated containing information showing site proposed enhancements with a proposal name, description of enhancement, rationale, impacts, costs, and milestone schedule. Information generated at the SMC will be accessed for use in this test procedure.

SMC-8800#A	This requirement is performed at the SMC using the office automation tools. This requirement is verified through test. The SMC shall have the capability to generate detailed and summary reports indicating the overall performance of the ECS. At a minimum, they include: a. Scheduled versus actual data collection, processing, retrieval, and delivery of routine data b. Scheduled versus actual data collection, processing, retrieval, and delivery of user requested data c. Reason(s) for failure to meet schedules d. Quality of the data e. Ground operations event execution f. Number of interactive user requests and timeliness of response g. User feedback The SMC must have the capability to produce standard or customized reports through use of the site report generator, from user requests through output to selected media. Information generated at the SMC will be accessed for use in this test procedure.
SMC-8820#A	This requirement is partially complied with at the SMC for this release, and is verified through test. The SMC shall have the capability to generate detailed and summary reports indicating the product generation status made in processing, reprocessing, and storage of all standard products. The SMC must have the capability to produce standard or customized reports through use of the site report generator, from user requests through output to selected media. Information generated at the SMC will be accessed for use in this test procedure.
SMC-8840#A	This requirement is performed at the SMC, and this requirement is verified through test. The SMC shall have the capability to generate detailed and summary reports indicating the performance of ground resources, including, at a minimum: a. Resource availability b. Reason for down time c. Resource utilization d. Ability of resource to meet performance criteria e. Short and long-term trend analysis and capacity planning results A report is generated showing the site performance of ground resources, including resource availability, reason for down time, resource utilization, the ability of resource to meet the performance criteria, and short and long-term trend analysis and capacity planning results. Information generated at the SMC will be accessed for use in this test procedure.
SMC-8841#A	This requirement is performed at the SMC using the office automation tools. This requirement is verified through test. The SMC shall have the capability to generate detailed and summary user feedback analysis reports describing the results of analyzing user satisfaction queries, including, at a minimum: a. User information b. Type of transaction c. Satisfaction statistics d. User recommendations

	e. SMC recommendations The SMC must have the capability to produce standard or customized reports through use of the site report generator, from user requests through output to selected media. Information generated at the SMC will be accessed for use in this test procedure.
SMC-8860#A	This requirement is performed at the SMC using the office automation tools. This requirement is verified through test. The SMC shall have the capability to generate detailed and summary fault management reports describing the fault management of ground resources, including, at a minimum: a. Fault type and description b. Time of occurrence of fault c. Effect on system d. Status of fault resolution e. Fault statistics A report is generated showing the site fault management reports describing the fault management of ground resources, including, fault type and description, time of occurrence of fault, effect on system, status of fault resolution, and fault statistics. Information generated at the SMC will be accessed for use in this test procedure.
SMC-8880#A	This requirement is performed at the SMC. Capabilities d, e, and g are performed by the M&O staff which generates reports using the office automation tools. Rest is automated. This requirement is verified through test. The SMC shall have the capability to generate detailed and summary security compromise reports indicating security compromises of ground resources and facilities, including, at a minimum: a. Security compromise type and description b. Time of occurrence c. Cause of security compromise d. Impact on system e. Status of security compromise resolution f. Security compromise statistics g. Results of security compromise risk analysis A report is generated showing the site security compromise reports indicating security compromises of ground resources and facilities, including, security compromise type and description, time of occurrence, cause of security compromise, impact on system, status of security compromise resolution, security compromise statistics, and results of security compromise risk analysis. Information generated at the SMC will be accessed for use in this test procedure.

Test Inputs: Specifications for the as-built report generator for the LSM.

Data Set Name	Data Set ID	File Name	Description	Version

Step-By-Step Procedures		
Step No.	**Input Action / Expected Results**	**Pass / Fail / Comments**
10	Production Monitor-QA: Verify that there is a fully operational site computer configuration.	
20	Production Monitor-QA: Verify that the site report generator and input data sets are available for access.	
30	Expected Results: Data sets representative of the full range of data types are available to be operated on by the report generator.	
40	Production Monitor-QA: Request use of the site report generator to produce a standard report.	
50	Expected Results: Display of steps involved in producing standard or customized reports through use of the site report generator, from user request through output to selected media.	
60	Production Monitor-QA: Define a report that generates detailed and summary information on training programs, training course schedules, training course contents, training course locations, and training attendees.	
70	Expected Results: Output includes a complete demonstration report that compares with the expected information.	
80	Production Monitor-QA: The output format is evaluated for correctness as well as readability and satisfactory presentation.	
90	Production Monitor-QA: Define a report that generates summary information showing the site inventory of hardware, system and scientific software, and spares and consumables.	
100	Expected Results: Output includes a complete demonstration report .	
110	Production Monitor-QA: The output format is evaluated for correctness as well as readability and satisfactory presentation.	
120	Production Monitor-QA: Define a report that generates information showing site proposed enhancements with a proposal name, description of enhancement, rationale, impacts, costs, and milestone schedule.	
130	Expected Results: Output includes a complete demonstration report .	
140	Production Monitor-QA: The output format is evaluated for correctness as well as readability and satisfactory presentation.	
150	Production Monitor-QA: Define a report that generates information showing the site performance of ground resources, including resource availability, reason for down time, resource utilization, the ability of resource to meet the performance criteria, and short and long-term trend analysis and capacity planning results.	

160	Expected Results: Output includes a complete demonstration report .	
170	Production Monitor-QA: The output format is evaluated for correctness as well as readability and satisfactory presentation.	
180	Production Monitor-QA: Define a report that generates information showing the site fault management reports describing the fault management of ground resources, including, fault type and description, time of occurrence of fault, effect on system, status of fault resolution, and fault statistics.	
190	Expected Results: Output includes a complete demonstration report .	
200	Production Monitor-QA: The output format is evaluated for correctness as well as readability and satisfactory presentation.	
210	Production Monitor-QA: Define a report that generates information showing the site security compromise reports indicating security compromises of ground resources and facilities, including, security compromise type and description, time of occurrence, cause of security compromise, impact on system, status of security compromise resolution, security compromise statistics, and results of security compromise risk analysis.	
220	Expected Results: Output includes a complete demonstration report .	
230	Production Monitor-QA: The output format is evaluated for correctness as well as readability and satisfactory presentation.	
240	Production Monitor-QA: Each of the previous report demonstrations is evaluated for adherence to report format and content specifications.	
250	Expected Results: The outputs include completed demonstration reports that compare expected versus actual outputs.	

Data Reduction and Analysis Steps:

A fully operational SMC computer configuration is required, ready to produce the specified reports including input data sets that are representative of nominal and special cases for each of the required report formats.

A. Evaluating report capabilities include generation of:

1. a functional allocation report giving the current allocation of ground segment functions;
2. summary configuration status reports;
3. summary training reports;
4. hardware, system and scientific software reports;
5. spares and consumables reports;
6. ground resources performance reports;
7. fault management reports; and
8. security compromise reports.

Signature:	**Date:**